



(19)

(11) Publication number:

09212457 A

Generated Document

## PATENT ABSTRACTS OF JAPAN

(21) Application number: 08014221

(51) Int. Cl.: G06F 15/00 G06F 13/00 G09C 1/00 G09C  
1/00 G09C 1/00 H04H 1/02 H04L 9/08  
H04L 9/32 H04N 7/14 H04N 7/167

(22) Application date: 30.01.96

(30) Priority:

(43) Date of application publication: 15.08.97

(84) Designated contracting states:

(71) Applicant: MITSUBISHI ELECTRIC CORP

(72) Inventor: OGAWA AKI

(74) Representative:

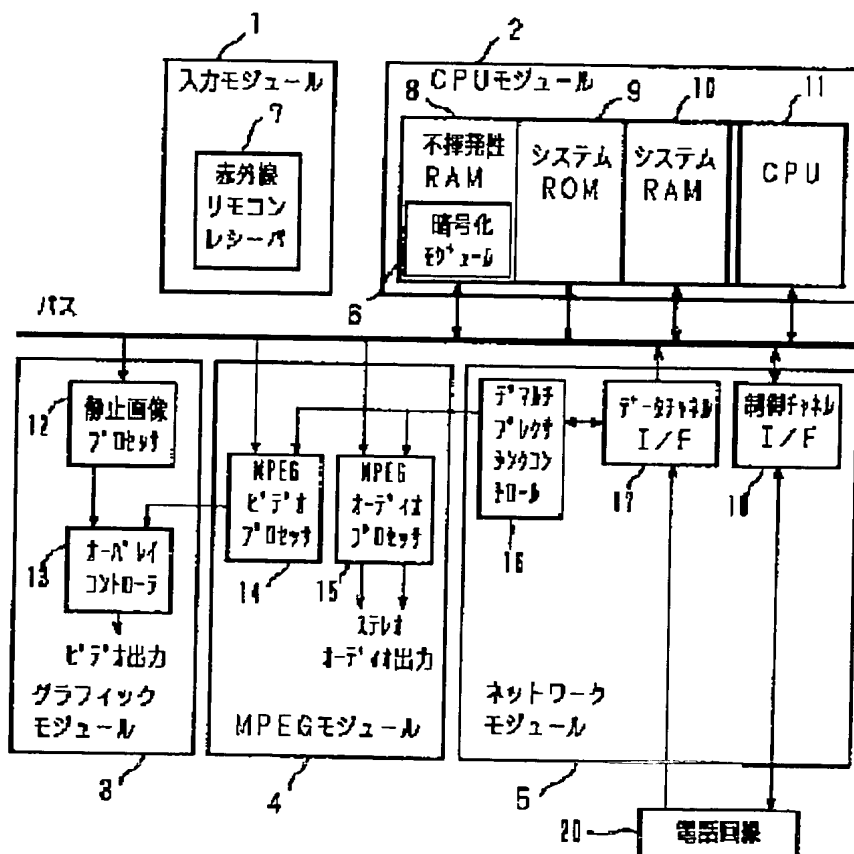
(54) CIPHERING AND  
DECIPHERING DEVICE OF  
DIGITAL BIDIRECTIONAL  
COMMUNICATION TERMINAL

(57) Abstract:

**PROBLEM TO BE SOLVED:** To keep the price of a digital bilateral communication terminal main body low by adding a ciphering, a deciphering, and a user authenticating function to a digital bilateral communication terminal, and then actualizing services which require security like credit card payment by bilateral CATV and further not incorporating the ciphering function originally, but downloading a ciphering module from a server.

**SOLUTION:** The digital bilateral communication terminal is connected to the server through a public telephone line or leased line and has a system ROM 9, a system RAM 10, and a nonvolatile RAM 8 inside and also has an operating system based upon OS/9. The digital bilateral communication terminal downloads modules for ciphering and deciphering data from the server, saves the downloaded ciphering module in the system RAM 10, and uses ciphering for the subsequent transmission and reception of data.

COPYRIGHT: (C)1997,JPO



(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-212457

(43) 公開日 平成9年(1997) 8月15日

(51) IntCl. <sup>9</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0		G 0 6 F 15/00	3 3 0 A
	3 5 1			3 5 1 H
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 C
		7259-5 J		6 3 0 E
	6 4 0	7259-5 J		6 4 0 B
審査請求 未請求 請求項の数 6 O L (全 49 頁) 最終頁に続く				

(21) 出願番号 特願平8-14221

(22) 出願日 平成8年(1996) 1月30日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 小川 亜紀

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

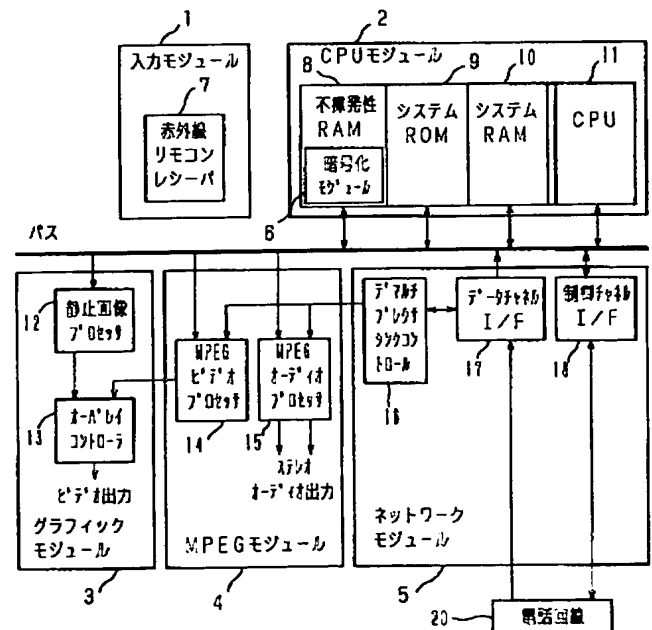
(74) 代理人 弁理士 宮田 金雄 (外3名)

## (54) 【発明の名称】 デジタル双方向通信端末における暗号化・復号化装置

## (57) 【要約】

【課題】 デジタル双方向通信端末において、デジタル双方向通信端末に暗号化、復号化およびユーザーの認証機能を付加することにより、双方向CATVによるクレジットカード支払い等のセキュリティを要するサービスの実現を可能とし、更に暗号化機能を初めから組み込むのではなく、暗号化モジュールをサーバからダウンロードさせることによって、デジタル双方向通信端末本体の価格を低く押さえることを可能とする。

【解決手段】 デジタル双方向通信端末は、公衆回線または専用線を通じてサーバに接続され内部にシステムROM、システムRAM、不揮発性RAMを有し、OS/9を核とするオペレーティングシステムを持つ。デジタル双方向通信端末はサーバよりデータの暗号化、復号化のためのモジュールをダウンロードし、ダウンロードした暗号化モジュールをシステムRAMに保存し、それ以降のデータの授受に暗号を使用する機能を有する。



## 【特許請求の範囲】

【請求項1】 公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にROM、不揮発性RAMとRAMを有し、OS/9（登録商標）を核とするオペレーティングシステムを持つデジタル双方向通信端末において、ドライバまたはアプリケーションはS/Wプログラムであり、特にCRCチェックコードを有する実行モジュール（以下、S/Wモジュール）であって、あらかじめ前記ROMに格納されているか、もしくはサーバよりダウンロードされ前記RAMに記憶され、初期化・リンクされることによって使用可能となるものであり、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記RAMに格納し、前記デジタル双方向通信端末と前記サーバ間で授受されるデータの暗号化、復号化機能を実現することを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項2】 公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にROM、不揮発性RAMとRAMを有し、OS/9を核とするオペレーティングシステムを持ち、H/Wによるデータの認証装置を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはS/Wプログラムであり、特にCRCチェックコードを有する実行モジュール（以下、S/Wモジュール）であって、あらかじめ前記ROMに格納されているか、もしくはサーバよりダウンロードされ前記RAMに記憶され、初期化・リンクされることによって使用可能となるものであり、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記RAMに格納し、前記デジタル双方向通信端末と前記サーバ間で授受されるデータの暗号化、復号化機能を実現し、前記認証装置によって、データの認証を行うことを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項3】 公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にROM、不揮発性RAMとRAMを有し、OS/9を核とするオペレーティングシステムを持ち、前記ROM内にデータの認証機能を実現するモジュール（以下、認証モジュール）を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはS/Wプログラムであり、特にCRCチェックコードを有する実行モジュール（以下、S/Wモジュール）であって、あらかじめ前記ROMに格納されているか、もしくはサーバよりダウンロードされ前記RAMに記憶され、初期化・リンクされることに

よって使用可能となるものであり、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記RAMに格納し、前記デジタル双方向通信端末と前記サーバ間で授受されるデータの暗号化、復号化機能を実現し、前記認証モジュールによって、データの認証を行うことを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項4】 公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にROM、不揮発性RAMとRAMを有し、OS/9を核とするオペレーティングシステムを持ち、前記ROM内にデータの認証機能を実現するモジュール（以下、認証モジュール）を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはS/Wプログラムであり、特にCRCチェックコードを有する実行モジュール（以下、S/Wモジュール）であって、あらかじめ前記ROMに格納されているか、もしくはサーバよりダウンロードされ前記RAMに記憶され、初期化・リンクされることによって使用可能となるものであり、暗号化・復号化機能は、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記RAMに格納し、前記デジタル双方向通信端末と前記サーバ間で授受されるユーザによる入力によって選択されたデータの暗号化、復号化機能を実現することを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項5】 公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にROM、不揮発性RAMとRAMを有し、OS/9を核とするオペレーティングシステムを持ち、前記ROM内にデータの認証機能を実現するモジュール（以下、認証モジュール）を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはS/Wプログラムであり、特にCRCチェックコードを有する実行モジュール（以下、S/Wモジュール）であって、あらかじめ前記ROMに格納されているか、もしくはサーバよりダウンロードされ前記RAMに記憶され、初期化・リンクされることによって使用可能となるものであり、暗号化・復号化機能は、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記RAMに格納し、前記サーバから前記デジタル双方向通信端末にダウンロードされた暗号化適用データリストに含まれるデータが前記デジタル双方向通信端末と前記サーバ間で授受される際の暗号化、復号化機能を実現することを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項6】 公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供

装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にROM、不揮発性RAMとRAMを有し、OS/9を核とするオペレーティングシステムを持ち、前記ROM内にデータの認証機能を実現するモジュール（以下、認証モジュール）を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはS/Wプログラムであり、特にCRCチェックコードを有する実行モジュール（以下、S/Wモジュール）であって、あらかじめ前記ROMに格納されているか、もしくはサーバよりダウンロードされ前記RAMに記憶され、初期化・リンクされることによって使用可能となるものであり、暗号化・復号化機能は、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記RAMに格納し、データが前記デジタル双方向通信端末と前記サーバ間で授受される際の暗号化、復号化機能を実現し、一度暗号化したデータの暗号化形式を前記RAM内に保持し、同じデータの送信時には記憶されたデータを使用する機能を有することとを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明はデジタル双方向通信端末にセキュリティ機能を付加するものであり、特にOS/9のモジュール形式と、双方向CATVシステムにおけるデータのダウンロード機能を利用して、暗号化機能を実現するデジタル双方向通信端末に関するものである。

##### 【0002】

【従来の技術】デジタル双方向通信端末用OSとしてOS/9を核としたDAVIDが発表されており、デジタル双方向通信端末を構成する最小限のモジュールによる構成とその拡張は既にDAVIDシステムとして発表されている。DAVIDと一般的なSTBの構造は日経バイト1995.9月号で解説されている。従来のデジタル双方向通信端末の構成と動作の詳細は後に記述する。しかし、DAVIDを含む典型的なデジタル双方向通信端末の構成には暗号化機能は含まれていない。拡張として暗号・条件付きアクセスの実現が取り上げられているが、ここでのセキュリティ機能は暗号化のためのH/WとH/Wに対応するドライバを組み込むことで実現されるものである。

【0003】従来のCATVシステムのセンターのサーバと端末装置とのデータの送受信方式については、特開昭57-65982号公報および特表平6-501601号公報に記述されているが、ここで送受信されるデータは暗号化が施されたものではなく、データに識別のためのコードを付加し、平文のままデータを流すものである。CATVシステムにおけるセキュリティとしては、ダウンロードされたブートイメージに含まれたデータ

から計算されたブーターチェックサムとプログラムのタグ信号から検出された有効チェックサムを比較し、一致すればデスクランブルが作動し、受信されるべきプログラムが視聴のためデスクランブルされる方式は特開昭63-26093号公報に記述されている。しかし、これはサーバから流れるデータを正当な視聴者にのみ受信可能となるよう視聴者を制限するためのものであり、視聴者側かのデータを保護するものではない。デジタル双方向通信端末において、双方向のデータを暗号化し、データ保護を実現するためには、暗号化・復号化装置が必要となる。

【0004】図40はOS/9を核とした一般のデジタル双方向通信端末の構成図である。図5において、1から5はそれぞれデジタル双方向通信端末におけるモジュールである。モジュールとは、ハードウェアとソフトウェアの組み合わせによって、デジタル双方向通信端末において各機能を実現するための構成要素であり、各モジュール間をバスを通じて制御信号、またはデータを送受信することによって、デジタル双方向通信端末を動作させるものである。以下、図40の構成要素を説明する。入力モジュール1、CPUモジュール2、グラフィックモジュール3、MPEGモジュール4、ネットワークモジュール5はそれぞれバスに接続されており、MPEGモジュール4はネットワークモジュール5の後段に配し、グラフィックモジュール3の前段に配している。入力モジュール1はユーザからの入力を受け付け、デジタル双方向通信端末内部に入力信号を取り込み、CPUへ信号送信を行うモジュールである。CPUモジュール2は中央処理装置と記憶装置からなるデジタル双方向通信端末内部の各モジュールからの信号を受け付け、受け付けた信号を処理し、必要なモジュールへ動作命令の出力を行い、それぞれのモジュールの制御を行うモジュールである。グラフィックモジュール3はサーバからダウンロードされた静止画像をビデオ出力可能な形式にデータ処理を行い、ビデオ出力へ出力させることと、MPEGモジュールから送られてきたデータをビデオ出力へ出力させることと、静止画像と動画像の重ね合わせ処理を行い、ビデオ出力へ出力させるモジュールである。MPEGモジュール4はネットワークモジュールより受信したサーバからダウンロードされたMPEGデータの復号を行い、オーディオデータをオーディオ出力に出力させることと、ビデオデータをグラフィックモジュールへ送信するモジュールである。ネットワークモジュール5はネットワークに接続され、ネットワークからデータを受信し、受信データを動画像・静止画像に分解し、更に動画については音声データとビデオデータに分解したあと、MPEGモジュールへデータを送信する処理を行うモジュールである。入力モジュールには、赤外線リモコンレシーバが含まれる。このレシーバによって、ユーザのリモコン操作による入力を受信し、デジタル双方向通信

端末へ取り込むことを可能とする。CPUモジュールにはCPU11、不揮発性RAM8、システムROM9、システムRAM10が存在する。CPUはデジタル双方向通信端末に取り込まれる信号を解析し、その解析結果に基づいて各モジュールへ動作命令信号を送信する。システムROMは、デジタル双方向通信端末本体に予め組み込まれるソフトウェアモジュールが記憶される。

【0005】図37に示すようにシステムROMには、OS-9のKernel26、I/Oマネージャ27、デバイスドライバ28、APIおよびプロトコル29が組み込まれ、アプリケーション領域30に、拡張されたアプリケーションモジュールを格納させることが可能である。システムRAM10および不揮発性RAM8には、STBの起動後にサーバからダウンロードされたデバイスドライバ、アプリケーション、データが記録される。グラフィックモジュールには、静止画像データを出力可能な形式に処理する静止画像プロセッサ12と、静止画像と、ビデオデータを取り込んで、重ね合わせなどの処理を行い、ビデオ出力に出力させるオーバレイコントローラ13が含まれる。MPEGモジュールには、ビデオデータとオーディオデータに切り分けられたMPEGデータのうち、ビデオデータを復号し、グラフィックモジュール内のオーバレイコントローラへ引き渡すMPEGビデオプロセッサ14と、オーディオデータを復号し、ステレオオーディオ出力に出力するMPEGオーディオプロセッサ15が含まれる。ネットワークモジュールには高帯域単方向回線に接続され、サーバからダウンロードされる画像データおよび音声データなどのデータを受信するためのデータチャンネルI/F17と、低帯域双方向回線とに接続され、通信制御を行うための信号を送受信し、デジタル双方向通信端末からサーバへの要求信号を送信し、サーバからの制御信号を受信するための制御チャンネルI/F18と、データチャンネルI/F17とデータの送受信を行い、MPEGデータのビデオデータとオーディオデータの切り分けを行い、MPEGオーディオプロセッサ15とMPEGビデオプロセッサ14への送信を行うデマルチプレクサシンクコントロール16が存在する。

【0006】次に、図40に示すデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。図38は電源ON時のデジタル双方向通信端末の動作フローチャートである。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、

Kernelの立ち上げを実行する。Kernelの立ち上げが終了した状態で、電源ON動作が完了する。

【0007】次に、ユーザからデータダウンロードのための選択信号入力があったときの動作を説明する。図39はデータダウンロード時のデジタル双方向通信端末の動作フローチャートである。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャンネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、データチャンネルI/F17を通じて、サーバからデータをダウンロードする。ダウンロードされたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバレイコントローラ13へ受け渡される。オーバレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上、従来のOS/9を核とした採用したデジタル双方向通信端末の動作を説明した。

【0008】

【発明が解決しようとする課題】上述した従来技術におけるネットワークセキュリティ技術はコンピュータネットワークにおける技術であり、双方向CATVシステムにおいてはまだ確立されていない。また、インターネット接続を実現するCATVにおいて、ケーブルモデムにセキュリティ機能を実装することが計画されているが、ケーブルモデムによるセキュリティ機能の実現であり、デジタル双方向通信端末そのものにセキュリティ機能を実装するものではなく、双方向CATVシステム単独でのセキュリティ機能ではない。しかし、オンライン

・ショッピングや銀行口座の残高照会といったサービスの提供を実現するためには双方向CATVシステムにおけるセキュリティ確保は必修条件である。双方向CATVでも、暗号化技術を取り入れたデジタル双方向通信端末を実現することによって、サーバ・端末間で送受信されるデータのセキュリティを確保することが可能であり、提供可能なサービスの幅を広げることができる。DAVIDの拡張としてセキュリティ機能が挙げられているが、これは暗号化のためのH/WとH/Wに対応するためのドライバを組み込むことによってデジタル双方向通信端末にセキュリティ機能を実現するものであり、デジタル双方向通信端末のH/W構成の変更を要し、一度組み込まれた暗号化方式を変更するためには更にH/Wの変更を必要とするものであり、暗号化のためのコストが高くなるという課題を有するものである。

【0009】本発明は上記のような課題を解決するためになされたもので、特にデジタル双方向通信端末にH/Wによるセキュリティ機能を組み込むのではなく、暗号化のためのアプリケーションモジュールとしてサーバからダウンロードさせることによって、暗号化機能付加のためのコストを軽減し、また暗号化機能の更新を容易に実現することができるデジタル双方向通信端末における暗号化・復号化装置を得ることを目的とする。

【0010】

【課題を解決するための手段】双方向CATVシステムにおける暗号化機能を実現するため、デジタル双方向通信端末に暗号化機能を実装する。暗号化機能としては、DES暗号に代表される秘密鍵暗号方式と、RSAに代表される公開鍵暗号方式を組み合わせた方式を用いるものとする。秘密鍵暗号方式とは、暗号化と復号化に用いる鍵が共通であり、暗号化に用いられた鍵を用いて暗号化アルゴリズムを逆に実行することによって、復号を行い、暗号化を施す前の原文を得るものである。この方式は、単純な排他的論理和の繰り返しアルゴリズムで実現されるもので、高速な処理を可能とする反面、送信側と受信側で共通の鍵を保有する必要がある、鍵の配送・保持が困難であるという欠点を有する。公開鍵暗号方式とは、落とし戸関数と呼ばれる一方向には容易に実行でき、逆数を求めるのは非常に困難である関数を利用するもので、暗号化と復号化に使用する鍵が異なるものである。したがって、鍵の配送・保持は容易に行える反面、秘密鍵暗号方式に比べて計算が複雑であり、秘密鍵暗号方式と比較して暗号化・復号化に処理時間を要するという欠点を有する。ただし、公開鍵暗号方式を使用して、認証及び鍵配送を行い、データの暗号化は秘密鍵暗号によって行うことによって、それぞれの利点を生かして使用することが可能となる。本発明に係るデジタル双方向通信端末における暗号化・復号化装置は、双方向CATVのデータダウンロード機能を活用し、暗号化のためのS/Wモジュールをサーバからダウンロードすることに

より、デジタル双方向通信端末に暗号化機能を組み込むとともに、モジュールをリンクし、デジタル双方向通信端末における暗号化機能を実現するものである。OS/9はデバイスドライバからアプリケーションに至るまで実行プログラムがそれぞれモジュールとなっており、それらモジュールをメモリにロードし、リンクすることにより、各種の機能をダイナミックに実行可能にすることができる特徴を持っている。このようなOS/9を核とするデジタル双方向通信端末では、各種の機能を実現するためのモジュールを予めROMに記憶させておく以外に、モジュールをサーバからダウンロードすることによってモジュールの機能をデジタル双方向通信端末に付加することが可能である。モジュールのダウンロードは通常デジタル双方向通信端末がサーバからオーディオデータ、ビデオデータ等をダウンロードするための回線を使用し、OS/9を核とするデジタル双方向通信端末のために開発されたデータのダウンロードプロトコル、UPLINK/DOWNLINK APIを使用する。デジタル双方向通信端末にはこのプロトコルモジュールを実装する。このダウンロードプロトコルは、サーバ用にはCライブラリが存在しており、任意のOS上で動作する。したがって、UPLINK/DOWNLINKプロトコルを使用した任意のOSを使用するサーバからのデータのダウンロードが可能である。

【0011】また、双方向CATVのデータダウンロード機能を活用し、暗号化のためのS/Wモジュールをサーバからダウンロードするとともに認証機能のためのH/Wを付加し、H/W認証装置のためのドライバをROMに組み込むものである。

【0012】また、双方向CATVのデータダウンロード機能を活用し、暗号化のためのS/Wモジュールをサーバからダウンロードするとともに、認証機能実現のための手段として、認証のためのS/Wモジュールは組み込みモジュールとしてROMに組み込むものである。

【0013】また、双方向CATVのデータダウンロード機能を活用し、暗号化のためのS/Wモジュールをサーバからダウンロードするとともに、ユーザの選択を受信するための手段として、リモコンを使用し、入力モジュールに暗号化を行うかどうかの選択信号を入力するための機能と、受信した選択信号をCPUモジュールに伝えるための機能を付加し、CPUモジュールのRAM領域に、選択信号を格納するための領域を確保するものである。

【0014】また、サーバからダウンロードしたリストを参照して選択的に暗号化を行うための手段として、双方向CATVのデータダウンロード機能を活用し、暗号化適用データのリストを参照して選択的に暗号化を行う機能を付加した暗号化のためのS/Wモジュールをサーバからダウンロードするとともにサーバから暗号化適用データのリストをダウンロードする機能と、暗号化適用データのリストを格納するための領域をRAM領域に設

けることとしたものである。

【0015】また、一度暗号化を実行したデータの暗号化形式を記憶し、同じデータの送信時に記憶されたデータを使用するために、双方向CATVのデータダウンロード機能を活用し、暗号化データのリストを参照し、暗号化データが存在しない場合にのみ選択的に暗号化を行う機能を付加した暗号化のためのS/Wモジュールをサーバからダウンロードするとともに、暗号化データの保存のための領域をRAM領域に設けることとしたものである。

【0016】

【発明の実施の形態】本発明の実施の形態であるデジタル双方向通信端末における暗号化・複号化装置においては、デジタル双方向通信端末に暗号化機能をダウンロードすることによって暗号化・複号化機能を実現させることが可能となるばかりでなく、データと同様にアプリケーションをダウンロードすることが可能であり、更にダウンロードされたアプリケーションをダイナミックに動作可能とするOS/9の特徴を利用した暗号化・複号化機能が実現できる。

【0017】また、認証機能のH/Wによる実装を行い、ユーザの認証を行うことによって、データの改ざん、不正なユーザによるなりすましを防ぐことができる。

【0018】また、認証機能のS/Wによる実装を行うことによって、ユーザの認証を実現し、データの改ざんや不正ユーザによるなりすましを防ぐことができる。

【0019】また、特にセキュリティの確保を必要とするデータを選択的に暗号化・複号化する機能を付加することによって、暗号化を必要としないデータをそのまま送受信することが可能となる。

【0020】また、データが暗号化・複号化を必要とするか否かをサーバ側で決定し、そのリストをデジタル双方向通信端末にダウンロードしてサーバ側と端末側で共通のリストによって、暗号化・複号化を選択的に実行する機能を有することによって、ユーザの操作が不要となり、ユーザの操作の煩雑さをなくすと共に、ユーザによる誤操作の危険性を回避でき、さらに暗号化・複号化は共通なリストによって選択するため、データが暗号化されたものであるかどうかを示すフラグを送受信されるデータに付加する必要がなくなる。

【0021】また、同じデータを何度も暗号化する必要がなくなり、デジタル双方向通信端末の負荷を軽減できる。

【0022】以下、本発明をその実施の形態を示す図面に基づいて説明する。

実施の形態1. 図1は本発明の実施の形態1であることを示すブロック図である。本実施の形態1において、ネットワークインターフェースモジュールはADSL対応であり、電話回線6に接続される。1から5の各モジュール

は従来例で示したものと同様であり、その機能も図40を用いて説明した従来ものと同様である。ただし、図1では、CPUモジュール2の不揮発性RAM8にダウンロードされる暗号化モジュールが格納される。

【0023】次に、本実施例におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。図2は実施例1における電源ON時のデジタル双方向通信端末の動作フローチャートである。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、Kernelの立ち上げを実行する。Kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。図5に電話回線を介したサーバとデジタル双方向通信端末の接続図を示し、ダウンロードを行う際の暗号化モジュールの流れを示す。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS 33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000（登録商標）39上のダウンロードプロトコルであるUPLINK/DOWNLINK APIを使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0024】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末

は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0025】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図3は実施の形態1におけるデータダウンロード時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャンネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図5に示した場合と同様にサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0026】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマル

チプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバレイコントローラ13へ受け渡される。オーバレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0027】図4は実施の形態1におけるデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、電話回線を経由して、サーバに送信される。データの送信は図5に示す様に、OS-90/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、電話回線36に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサ



サーバへデータを安全に送信することが可能となる。

【0028】実施の形態2．本実施の形態2において、ネットワークインターフェースモジュールはHFC対応である。図6はネットワークインターフェースモジュールとしてHFCを使用する場合のブロック図、図7はサーバとデジタル双方向通信端末の接続図である。図7および図4に示すように、デジタル双方向通信端末はネットワークインターフェースモジュールから同軸ケーブル44、ファイババックボーン42を経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0029】次に、本実施の形態2におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態2における電源ON時のデジタル双方向通信端末の動作フローチャートは図2と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、Kernelの立ち上げを実行する。Kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。図7にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示す。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42を通して、ファイバと同軸ケーブルを接続するファイババックボーン43を経由し、同軸ケーブル44に接続されているデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0030】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い

暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0031】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。実施の形態2における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は図3と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図7に示したサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42へ送信され、さらにファイババックボーン43を経由し、同軸ケーブル44を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0032】ダウンロードされたデータはCPUモジュール

ール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバーレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバーレイコントローラ13へ受け渡される。オーバーレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0033】実施の形態2における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作は図4と同様である。まず、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、同軸ケーブル44から送信され、ファイババックボーン43、ファイバケーブル44を経由して、サーバに送信される。データの送信は図7に示す様に、OS-9/OS¥9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、同軸ケーブル44に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLI

NK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42よりデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となる。

【0034】実施の形態3. 本実施の形態3において、ネットワークインターフェースモジュールはATM対応である。図8はネットワークインターフェースモジュールとしてATMを使用する場合のブロック図、図9はATMネットワークを介して接続されるサーバとデジタル双方向通信端末間のデータの流れを示す図である。デジタル双方向通信端末はネットワークインターフェースモジュールからファイバケーブル46を経由し、ATMスイッチ45を介してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0035】次に、本実施の形態3におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態3における電源ON時のデジタル双方向通信端末の動作フローチャートは図2と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、Kernelの立ち上げを実行する。Kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。図9にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示す。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42を通して、ATMスイッチ45を経由し、ファイバケーブル46に接続されているデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバケーブル46に接続されているハードウ

エア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0036】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0037】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。実施の形態3における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は図3と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイ

バーケーブル42へ送信され、さらにATMスイッチ45を経由し、デジタル双方向通信端末に接続されたファイバーケーブル46よりデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0038】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバーレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバーレイコントローラ13へ受け渡される。オーバーレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0039】暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作は図4と同様である。まず、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用

暗号化鍵は、バスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、ATM9送信される。データの送信は図9に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、ファイバケーブル46に接続されているハードウェア37から送信され、ATMスイッチを経由してサーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42よりデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となる。

【0040】実施の形態4. 図10は本発明の実施の形態4であるシステム構成のブロック図である。本実施の形態において、ネットワークインターフェースモジュールはADSL対応であり、電話回線6に接続される。請求項2に記載されるデジタル双方向通信端末は認証・鍵配送のための暗号化モジュール（以下、H/W認証モジュール）をH/Wとして有しており、認識および鍵配送の暗号化処理にはH/W認証モジュールを使用する。

【0041】次に、本実施の形態の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。図11は実施の形態1における電源ON時のデジタル双方向通信端末の動作フローチャートである。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末のH/W認証モジュールによって、デジタル双方向通信端末固有のID、ユーザのアクセスID、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール6のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましが無いことを確認し、デジタル双方向通

信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図5と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0042】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図12はデータダウンロード時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、H/W認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をH/W認証モジュール10へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったH/W認証モジュール10は、認証のための暗号化を施し、ネットワークモジュール5へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャンネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密

鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図5に示した場合と同様にサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS 33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM 10に格納される。

【0043】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM 10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバレイコントローラ13へ受け渡される。オーバレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0044】図13はデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してH/W認証モジュール10へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったH/W認証モジュール10は、認証のための暗号化を施し、ネットワークモジュール5へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、電話回線を経由して、サーバに送信される。データの送信は図5に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS 33を介して、電話回線36に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36からデジタル双方向通信端末から送信されたデータを受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらにサーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましが無いことを確認することが可能となる。

【0045】実施の形態5．本発明の実施の形態3において、ネットワークインターフェースモジュールをHFC対応とすることができる。図14は本発明の実施の形態5であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてHFCを使用する場合を示す。デジタル双方向通信端末はネットワークインターフェースモジュールから同軸ケーブルからファイババックボーンを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0046】次に、本実施の形態3の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態5における電源ON時のデジタル双

方向通信端末の動作フローチャートは図11と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末のH/W認証モジュールによって、デジタル双方向通信端末固有のID、ユーザのアクセスID、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール6のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましが無いことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図7と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からファイババックボーン43を経由し、同軸ケーブル44に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0047】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図12と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、H/W認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をH/W認証モジュール10へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったH/W認証モジュール10は、認証のための暗号化を施し、ネットワークモジュール5へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図7に示した場合と同様にサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からファイババックボーン43を経由して同軸ケーブル44に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0048】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを適してグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デ

マルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバレイコントローラ13へ受け渡される。オーバレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0049】暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作のフローチャートは図13と同様である。まず、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してH/W認証モジュール10へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったH/W認証モジュール10は、認証のための暗号化を施し、ネットワークモジュール5へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、HFC8を経由して、サーバに送信される。データの送信は図11に示す様に、OS-9/OS-900039上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からファイババックボーン43を経由し、同軸ケーブルからデジタル双方向通信端末が送信した認証のための暗号化を施され、更に暗号化

されたデータとデータ用暗号化鍵を受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらにサーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましのないことを確認することが可能となる。

【0050】実施の形態6. 本発明の実施の形態3において、ネットワークインターフェースモジュールをATM対応とすることができる。図15は本発明の実施の形態6であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてATMを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールからATMを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0051】次に、本実施の形態6の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態6における電源ON時のデジタル双方向通信端末の動作フローチャートは図11と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末のH/W認証モジュールによって、デジタル双方向通信端末固有のID、ユーザのアクセスID、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール6のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましのないことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図9と同様である。サーバのアプリケーション



ン領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS 33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバーケーブル42からATMスイッチ45を経由し、ファイバーケーブル46に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM 8である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM 8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0052】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図12と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、H/W認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をH/W認証モジュール10へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったH/W認証モジュール10は、認証のための暗号化を施し、ネットワークモジュール5へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャネルI/F 18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図9に示した場合と同様にサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向

通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS 33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバーケーブル42からATMスイッチ45を経由してファイバーケーブル46に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM 10に格納される。

【0053】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM 10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバーレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバーレイコントローラ13へ受け渡される。オーバーレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0054】次に実施の形態6において、暗号化を施されたデータを送信する場合を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図13と同様である。まず、デジタル双方向通信端末はCPUモジュール2において、暗号化モジ



ジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してH/W認証モジュール10へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったH/W認証モジュール10は、認証のための暗号化を施し、ネットワークモジュール5へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、ATM9を経由して、サーバに送信される。データの送信は図9と同様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からATMスイッチ45を経由し、ファイバケーブル46からデジタル双方向通信端末が送信した認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信する。認証のための暗号化を施され、さらに暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらに、サーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましが無いことを確認することが可能となる。

【0055】実施の形態7. 図16は本発明の実施の形態7であるシステム構成を示すブロック図である。本実施の形態7において、ネットワークインターフェースモジュールはADSL対応であり、電話回線6に接続される。請求項2に記載されるデジタル双方向通信端末は認証・鍵配送のための暗号化モジュール（以下、S/W認証モジュール）をS/Wとして有しており、認証および鍵配送の暗号化処理にはS/W認証モジュールを使用する。S/W認証モジュールはシステムROMのアプリケーション領域に組み込まれる。

【0056】次に、本実施の形態7の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施例7における電源ON時のデジタル双方向通信端末の動作フローチャートは図11と同様である。

入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末のS/W認証モジュールによって、デジタル双方向通信端末固有のID、ユーザのアクセスID、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール6のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましが無いことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図5と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0057】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信に

ついて説明する。実施例7において暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は図12と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、S/W認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をS/W認証モジュール11へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったS/W認証モジュール11は、認証のための暗号化を施し、ネットワークモジュール5へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャンネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図5に示した場合と同様にサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0058】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ

受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバレイコントローラ13へ受け渡される。オーバレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0059】実施の形態7において、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作は図13と同様である。まず、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してS/W認証モジュール11へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったS/W認証モジュール11は、認証のための暗号化を施し、ネットワークモジュール5へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、電話回線を経由して、サーバに送信される。データの送信は図5に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、電話回線36に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36からデジタル双方向通信端末から送信されたデータを受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらに、サーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化

鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましが無いことを確認することが可能となる。

【0060】実施の形態8. 本発明の実施の形態3において、ネットワークインターフェースモジュールをHFC対応とすることができる。図17は実施の形態8であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてHFCを使用する場合を示す。デジタル双方向通信端末はネットワークインターフェースモジュールから同軸ケーブルからファイババックボーンを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0061】次に、本実施の形態8の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態8における電源ON時のデジタル双方向通信端末の動作フローチャートは図11と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末のS/W認証モジュールによって、デジタル双方向通信端末固有のID、ユーザのアクセスID、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール6のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましが無いことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図7と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバ

ケーブル42からファイババックボーン43を経由し、同軸ケーブル44に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。次に、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0062】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。実施の形態8において暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図12と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、S/W認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をS/W認証モジュール11へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったS/W認証モジュール11は、認証のための暗号化を施し、ネットワークモジュール5へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図7に示した場合と同様にサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からファイババックボーン43を経

由して同軸ケーブル44に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK APIを使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0063】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバーレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバーレイコントローラ13へ受け渡される。オーバーレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0064】実施の形態8における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図13と同様である。まず、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バ

スを介してS/W認証モジュール11へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったS/W認証モジュール11は、認証のための暗号化を施し、ネットワークモジュール5へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、HFC8を経由して、サーバに送信される。データの送信は図7に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からファイババックボーン43を経由し、同軸ケーブルからデジタル双方向通信端末が送信した認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらにサーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましが無いことを確認することが可能となる。

【0065】実施の形態9. 本発明の実施の形態7において、ネットワークインターフェースモジュールをATM対応とすることができる。図18は実施の形態9であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてATMを使用する場合を示す。デジタル双方向通信端末はネットワークインターフェースモジュールからATMを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0066】次に、本実施の形態9の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態9における電源ON時のデジタル双方向通信端末の動作フローチャートは図11と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、

システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末のS/W認証モジュールによって、デジタル双方向通信端末固有のID、ユーザのアクセスID、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール6のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましがいないことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図9と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバーケーブル42からATMスイッチ45を経由し、ファイバーケーブル46に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0067】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図12と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロー

ドすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、S/W認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をS/W認証モジュール11へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったS/W認証モジュール11は、認証のための暗号化を施し、ネットワークモジュール5へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャンネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図9に示した場合と同様にサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバーケーブル42からATMスイッチ45を経由してファイバーケーブル46に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0068】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバーレイ

コントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバーレイコントローラ13へ受け渡される。オーバーレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0069】暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図13と同様である。まず、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してS/W認証モジュール11へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったS/W認証モジュール11は、認証のための暗号化を施し、ネットワークモジュール5へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、HFC8を経由して、サーバに送信される。データの送信は図9に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS 33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からATMスイッチ45を経由し、ファイバケーブル46からデジタル双方向通信端末が送信した認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらにサーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末

はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましのないことを確認することが可能となる。

【0070】実施の形態10. 図19は本発明の実施の形態10であるシステム構成を示すブロック図である。本実施の形態において、ネットワークインターフェースモジュールはADSL対応であり、電話回線6に接続される。

【0071】次に、本実施の形態10であるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態10における電源ON時のデジタル双方向通信端末の動作フローチャートを図20に示す。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。図5にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示す。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS 33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0072】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信

されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0073】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図21はデータダウンロード時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。デジタル双方向通信端末は入力モジュール1からユーザによって入力された暗号化ON/OFF命令受信し、バスを通じてシステムRAM9に暗号化ON/OFFのフラグ（データ暗号化フラグ）を記憶する。本実施の形態10における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は、サーバへの要求にデータ暗号化フラグを添付すること以外は図2と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール5は制御チャネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側ではデータ暗号化フラグによって示されるデータ暗号化のON/OFFを確認し、データ暗号化がONである場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データの暗号化がOFFである場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。

【0074】データのダウンロードは図5に示した場合と同様にUPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・

マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。データ暗号化がONである場合、ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がOFFの場合は、復号化は省略される。受信されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバレイコントローラ13へ受け渡される。オーバレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0075】図22はデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はシステムRAMに記憶されたデータ暗号化フラグをチェックし、データ暗号化フラグがONである場合、送信しようとするデータの暗号化を実行する。データ暗号化フラグがONである場合、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用し



たデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、電話回線を経由して、サーバに送信される。データの送信は図5に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、電話回線36に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用し、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【0076】データ暗号化フラグがOFFである場合、サーバに送信すべきデータはバスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、電話回線を経由して、サーバに送信される。データの送信は図5に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、電話回線36に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0077】実施の形態11. 本実施の形態11において、ネットワークインターフェースモジュールはHFC対応である。図23は実施の形態11であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてHFCを使用する場合を示す。デジタル双方向通信端末はネットワークインターフェースモジュールから同軸ケーブルからファイババックボーン

を経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0078】次に、本実施の形態11におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態11における電源ON時のデジタル双方向通信端末の動作フローチャートは図20と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。図7にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示す。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からファイババックボーン43を経由して同軸ケーブル44からデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OA-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0079】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存す



る。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0080】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図21と同様である。デジタル双方向通信端末は入力モジュール1からユーザによって入力された暗号化ON/OFF命令を受信し、バスを通じてシステムRAM9に暗号化ON/OFFのフラグ（データ暗号化フラグ）を記憶する。本実施の形態11における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は、サーバへの要求にデータ暗号化フラグを添付すること以外は図6と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール5は制御チャンネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側ではデータ暗号化フラグによって示されるデータ暗号化のON/OFFを確認し、データ暗号化がONである場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データの暗号化がOFFである場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。

【0081】データのダウンロードは図7に示した場合と同様にUPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からファイババックボーン43を経由して同軸ケーブル44からデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。デ

ータ暗号化がONである場合、ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がOFFの場合は、復号化は省略される。受信されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバレイコントローラ13へ受け渡される。オーバレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0082】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図22と同様である。まず、デジタル双方向通信端末はシステムRAMに記憶されたデータ暗号化フラグをチェックし、データ暗号化フラグがONである場合、送信しようとするデータの暗号化を実行する。データ暗号化フラグがONである場合、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサ

サーバの公開鍵を用いて暗号化する。次に、デジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、同軸ケーブル44からファイババックボーン43、ファイバケーブル42を経由して、サーバに送信される。データの送信は図7に示す様に、OS-9/OS-900039上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている同軸ケーブル44を使用してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【0083】データ暗号化フラグがOFFである場合、サーバに送信すべきデータはバスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、同軸ケーブル44からファイババックボーン43、ファイバケーブル42を経由して、サーバに送信される。データの送信は図7に示す様に、OS-9/OS-900039上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている同軸ケーブル44からファイババックボーン43、ファイバケーブル42を経由してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0084】実施の形態12. 本実施の形態12において、ネットワークインターフェースモジュールはATM対応である。図24は実施の形態12であるシステム構

成を示すブロック図であり、ネットワークインターフェースモジュールとしてATMを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールから光ファイバケーブルを経由し、ATMスイッチを介してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0085】次に、本実施の形態12におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施例12における電源ON時のデジタル双方向通信端末の動作フローチャートは図20と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図9と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からATMスイッチ45を経由して、ファイバケーブル46からデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-900039上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0086】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信

したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0087】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図21と同様である。デジタル双方向通信端末は入力モジュール1からユーザによって入力された暗号化ON/OFF命令を受信し、バスを通じてシステムRAM9に暗号化ON/OFFのフラグ（データ暗号化フラグ）を記憶する。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール5は制御チャネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側ではデータ暗号化フラグによって示されるデータ暗号化のON/OFFを確認し、データ暗号化がONである場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データの暗号化がOFFである場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。

【0088】データのダウンロードは図9に示した場合と同様にUPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からATMスイッチ45からファイバケーブル46を経由してデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納され

る。データ暗号化がONである場合、ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がOFFの場合は、復号化は省略される。受信されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバーレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバーレイコントローラ13へ受け渡される。オーバーレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0089】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図22と同様である。まず、デジタル双方向通信端末はシステムRAMに記憶されたデータ暗号化フラグをチェックし、データ暗号化フラグがONである場合、送信しようとするデータの暗号化を実行する。データ暗号化フラグがONである場合、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバ

の公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、ファイバケーブル46からATMスイッチ45、ファイバケーブル42を経由して、サーバに送信される。データの送信は図9に示すのと同様に、OS-9/OS-9000

39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル46を使用してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【0090】データ暗号化フラグがOFFである場合、サーバに送信すべきデータはバスを介してネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、ファイバケーブル46からATMスイッチ45、ファイバケーブル42を経由して、サーバに送信される。データの送信は図9に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル46、ATMスイッチ45、ファイバケーブル42を経由してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0091】実施の形態13. 図25は本発明の実施の形態13であるシステム構成を示すブロック図である。本実施の形態13において、ネットワークインターフェ

ースモジュールはADSL対応であり、電話回線6に接続される。

【0092】次に、本実施の形態13におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態10における電源ON時のデジタル双方向通信端末の動作フローチャートを図26に示す。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6と暗号化を行うべきデータのリストである暗号化適用データリスト12のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納され、暗号化適用データリストはシステムRAM10に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図5と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0093】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末

は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0094】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図27はダウンロード時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。デジタル双方向通信端末は入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール5は制御チャンネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では要求されたデータが暗号化適用データリストに含まれるかどうかを確認し、送信すべきデータが暗号化適用データリストに含まれる場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。要求されたデータが暗号化適用データリストに含まれない場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。

【0095】データのダウンロードは図9に示した場合と同様にUPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。デジタル双方向通信端末は、暗号化適用データリスト12を参照し、ダウンロードしたデータが暗号化適用データリストに含まれる場合、ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵

を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がOFFの場合は、復号化は省略される。受信されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバレイコントローラ13へ受け渡される。オーバレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0096】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。図28はデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はシステムRAMに記憶された暗号化適用データリスト12を参照し、送信すべきデータが暗号化適用データリストに含まれる場合、送信しようとするデータの暗号化を実行する。データの暗号化を行う場合、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、電話回線を経

由して、サーバに送信される。データの送信は図5に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、電話回線36に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【0097】送信すべきデータが暗号化適用データリストに含まれない場合、サーバに送信すべきデータはバスを介してネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、電話回線を経由して、サーバに送信される。データの送信は図5に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、電話回線36に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36からデジタル双方向通信端末から送信されたデータを受信する。データを受信したサーバはデータが暗号化適用データリスト12に含まれないことを確認して、データはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0098】実施の形態14. 本実施の形態14において、ネットワークインターフェースモジュールはHFC対応である。図29は本発明の実施の形態14であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてHFCを使用する場合を示す。デジタル双方向通信端末はネットワークインターフェースモジュールから同軸ケーブルからファイババックボーンを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0099】次に、本実施の形態14におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態12における電源ON時のデジタル双方向通信端末の動

作フローチャートは図26と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行う電源ONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6と暗号化を行うべきデータのリストである暗号化適用データリスト12のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納され、暗号化適用データリストはシステムRAM10に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図9と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42、ファイババックボーン43、同軸ケーブル44を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK APIを使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0100】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が

行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0101】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図29と同様である。デジタル双方向通信端末は入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール5は制御チャンネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では要求されたデータが暗号化適用データリストに含まれるかどうかを確認し、送信すべきデータが暗号化適用データリストに含まれる場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。要求されたデータが暗号化適用データリストに含まれない場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。データのダウンロードは図7に示した場合と同様にUPLINK/DOWNLINK API 32を使用し、サーバ用のOS 33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42、ファイババックボーン43、同軸ケーブル44を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK APIを使用して、デジタル双方向通信端末のシステムRAM 10に格納される。

【0102】デジタル双方向通信端末は、暗号化適用データリスト12を参照し、ダウンロードしたデータが暗号化適用データリストに含まれる場合、ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM 10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗

号化がOFFの場合は、復号化は省略される。受信されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバレイコントローラ13へ受け渡される。オーバレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0103】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図28と同様である。まず、デジタル双方向通信端末はシステムRAMに記憶された暗号化適用データリスト12を参照し、送信すべきデータが暗号化適用データリストに含まれる場合、送信しようとするデータの暗号化を実行する。データの暗号化を行う場合、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、ファイバケーブル46からATMスイッチ45、ファイバケーブル42を経由して、サーバに送信される。データの送信は図7に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであ

るUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている同軸ケーブル44からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【0104】送信すべきデータが暗号化適用データリストに含まれない場合、サーバに送信すべきデータはバスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、ファイバケーブル46からATMスイッチ、ファイバケーブル42を経由して、サーバに送信される。データの送信は図9に示す様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からファイババックボーン43、同軸ケーブル44を経由してデジタル双方向通信端末から送信されたデータを受信する。データを受信したサーバはデータが暗号化適用データリスト12に含まれないことを確認して、データはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0105】実施の形態15. 本実施の形態15において、ネットワークインターフェースモジュールはATM対応である。図30は実施の形態15であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてATMを使用する場合を示す。デジタル双方向通信端末はネットワークインターフェースモジュールから光ファイバケーブルを経由し、ATMスイッチを介してサービスプロバイダのサービス提供装置であるサーバに接続される。

【0106】次に、本実施の形態15におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施N0形態15における電源ON時のデジタル双方向通信端末の

動作フローチャートは図26と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。図9にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示している。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42からATMスイッチ45を経由して、ファイバケーブル46からデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0107】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のように、デジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0108】次に、実行可能となった暗号化モジュール



を使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図29と同様である。デジタル双方向通信端末は入力モジュール1からユーザによって入力された暗号化ON/OFF命令受信し、バスを通じてシステムRAM9に暗号化ON/OFFのフラグ（データ暗号化フラグ）を記憶する。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール5は制御チャネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側ではデータ暗号化フラグによって示されるデータ暗号化のON/OFFを確認し、データ暗号化がONである場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データの暗号化がOFFである場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。データのダウンロードは図9に示した場合と同様にUPLINK/DOWNLINK API 32を使用し、サーバ用のOS 33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバーケーブル42からATMスイッチ45からファイバーケーブル46を経由してデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル46に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK APIを使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0109】データ暗号化がONである場合、ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がOFFの場合は、復号化は省略される。受信されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MP

EGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバーレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバーレイコントローラ13へ受け渡される。オーバーレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0110】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図28と同様である。まず、デジタル双方向通信端末はシステムRAMに記憶されたデータ暗号化フラグをチェックし、データ暗号化フラグがONである場合、送信しようとするデータの暗号化を実行する。データ暗号化フラグがONである場合、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次に、デジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。次に、デジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、ファイバーケーブル46からATMスイッチ45、ファイバーケーブル42を経由して、サーバに送信される。データの送信は図9に示した様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS 33を介して、ファイバーケーブル42に接続されているハードウェア3

7から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル46を使用してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【0111】データ暗号化フラグがOFFである場合、サーバに送信すべきデータはバスを介してネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、ファイバケーブル46からATMスイッチ45、ファイバケーブル42を経由して、サーバに送信される。データの送信は図9に示した様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用して、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【0112】実施の形態16、図31は実施の形態16であるシステム構成のブロック図である。本実施の形態16において、ネットワークインターフェースモジュールはADSL対応であり、電話回線6に接続される。また、システムRAM内に一度暗号化を施したデータを記憶しておくための領域（暗号化データ記憶領域13）を有する。

【0113】次に、本実施の形態16におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。図32はデジタル双方向通信端末電源ON時のフローチャートである。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジ

ュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図5と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0114】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0115】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図33はデータダウンロード時のフローチャートであり、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。入力モジュール1より、データダウンロード実行信号を受信したデジ

タル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図5に示した場合と同様にサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線36に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0116】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してデマルチプレクサシンクコントロール16へ受け渡される。デマルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバーレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバーレイコントロ

ーラ13へ受け渡される。オーバーレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0117】図34はデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はシステムRAM内の暗号化データ記憶領域13に、送信すべきデータの暗号化されたデータの検索を行う。暗号化データ記憶領域13に送信すべきデータが存在しない場合、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。デジタル双方向通信端末は暗号化を施したデータと暗号化に使用した暗号化鍵をシステムRAM10上の暗号化データ記憶領域13に格納する。暗号化データ記憶領域の要領を超える場合には、最終の参照日時が最も古いものから順にデータを消去する。暗号化データ記憶領域13に送信すべきデータが存在する場合、デジタル双方向通信端末はそのデータと暗号化鍵をサーバに送信する。

【0118】次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャネルI/Fへ送られ、制御チャネルI/Fを介して、電話回線を経由して、サーバに送信される。データの送信は図5に示した様に、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、電話回線36に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている電話回線36からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またデジタル双方向通信端末におけるデータの暗号化処理の必要回数を減らすことが可能となり、サーバへのデータ送

信の効率を上げることが可能となる。

【0119】実施の形態17. 図35は実施の形態17であるシステム構成を示すブロック図である。本実施の形態17において、ネットワークインターフェースモジュールはHFC対応であり、デジタル双方向通信端末は同軸ケーブル7に接続される。また、システムRAM内に一度暗号化を施したデータを記憶しておくための領域（暗号化データ記憶領域13）を有する。

【0120】次に、本実施の形態17におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態17における電源ON時のデジタル双方向通信端末の動作フローチャートは図32と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図7と同様である。サーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42、ファイババックボーン43を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域41に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域41は、不揮発性RAM8である。

【0121】暗号化モジュール6がダウンロードされ、不揮発性RAM8に格納されると、次にデジタル双方向通信端末は暗号化モジュール6の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムROM10のアプリケーション領域30に保存

されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、この受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域31に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性RAM8に保存する。以上のように、デジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール6のダウンロードを実行するデジタル双方向通信端末の電源ON動作が終了する。

【0122】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図33と同様である。入力モジュール1より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をCPUモジュール2へ受け渡す。ダウンロード命令を受信したCPUモジュールは、ネットワークモジュール5へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール5は制御チャネルI/F18を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図7に示した場合と同様にサーバのアプリケーション領域31に格納されている暗号化モジュール6は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 32を使用し、サーバ用のOS33を介して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバケーブル42、ファイババックボーン43を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル44に接続されているハードウェア37から、ファイル・マネージャ、ドライバ38によって、OS-9/OS-9000 39上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムRAM10に格納される。

【0123】ダウンロードされたデータはCPUモジュール2の暗号化モジュール6を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号

化鍵を復号する。復号されたデータ用暗号化鍵は、システムRAM10に保存される。次に復号され、システムRAMに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEGデータ以外のデータはバスを通じてグラフィックモジュール3へ送信され、MPEGデータはバスを介してマルチプレクサシンクコントロール16へ受け渡される。マルチプレクサシンクコントロール16に受け渡されたMPEGデータは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEGモジュール4へ受け渡される。MPEGモジュール4に受け取られた画像データはMPEGビデオプロセッサ14で、音声データはMPEGオーディオプロセッサ15でそれぞれ復号処理され、MPEGビデオプロセッサ14で復号されたビデオ信号は、グラフィックモジュール3のオーバーレイコントローラ13に受け渡され、MPEGオーディオプロセッサ15で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール3へ受け渡された静止画像データは静止画像プロセッサ12で復号処理され、オーバーレイコントローラ13へ受け渡される。オーバーレイコントローラ13では、静止画像プロセッサ12から受け取った静止画像データとMPEGビデオプロセッサ14から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0124】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図34と同様である。まず、デジタル双方向通信端末はシステムRAM内の暗号化データ記憶領域13に、送信すべきデータの暗号化されたデータの検索を行う。暗号化データ記憶領域13に送信すべきデータが存在しない場合、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。デジタル双方向通信端末は暗号化を施したデータと暗号化に使用した暗号化鍵をシステムRAM10上の暗号化データ記憶領域13に格納する。暗号化データ記憶領域の要領を超える場合には、最終の参照日時が最も古いものから順にデータを消去する。暗号化データ記憶領域13に送信すべきデータが存在する場合、デジタル双方向通信端末はそのデータと暗号化鍵をサーバに送信する。

【0125】次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、同軸ケーブル44、ファイバーバックボーン43を経由して、サーバに送信される。データの送信は図7と同様に、OS-9/OS-900039上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバーケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されている同軸ケーブル44からファイバーバックボーン43を経由してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またデジタル双方向通信端末におけるデータの暗号化処理の必要回数を減らすことが可能となり、サーバへのデータ送信の効率を上げることが可能となる。

【0126】実施の形態18. 図36は実施の形態18であるシステム構成を示すブロック図である。本実施の形態18において、ネットワークインターフェースモジュールはATM対応であり、デジタル双方向通信端末はファイバーケーブルに接続される。また、システムRAM内に一度暗号化を施したデータを記憶しておくための領域(暗号化データ記憶領域13)を有する。

【0127】次に、本実施の形態18におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施例18における電源ON時のデジタル双方向通信端末の動作フローチャートは図32と同様である。入力モジュール1より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ7で信号が電源ON信号であることを解析し、CPUへ電源ON信号を送信する。電源ON信号を受信したCPUモジュールは、各モジュール[1-5]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーONセルフテストを実行する。次に、システムROM9とシステムRAM10の初期化を行う。次に、kernelの立ち上げを実行する。kernelの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール6のダウンロードを行う。ダウンロードした暗号化モジュール6はアプリケーションとして不揮発性RAM8に格納される。ダウンロード

を行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図 9 と同様である。サーバのアプリケーション領域 3 1 に格納されている暗号化モジュール 6 は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 3 2 を使用し、サーバ用の OS 3 3 を介して、サーバ固有のネットワークドライバ 3 4 を使用して、ハードウェア 3 5 を介して接続されているファイバケーブル 4 2、ATM スイッチ 4 5 を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル 4 4 に接続されているハードウェア 3 7 から、ファイル・マネージャ、ドライバ 3 8 によって、OS-9/OS-9000 3 9 上のダウンロードプロトコルである UPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域 4 1 に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域 4 1 は、不揮発性 RAM 8 である。

【0128】暗号化モジュール 6 がダウンロードされ、不揮発性 RAM 8 に格納されると、次にデジタル双方向通信端末は暗号化モジュール 6 の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステム ROM 1 0 のアプリケーション領域 3 0 に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域 3 1 に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性 RAM 8 に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール 6 のダウンロードを実行するデジタル双方向通信端末の電源 ON 動作が終了する。

【0129】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図 3 3 と同様である。入力モジュール 1 より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名を CPU モジュール 2 へ受け渡す。ダウンロード命令を受信した CPU モジュールは、ネットワークモジュール 5 へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール 5 は制御チャネル I/F 1 8 を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送

を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図 1 3 に示した場合と同様にサーバのアプリケーション領域 3 1 に格納されている暗号化モジュール 6 は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API 3 2 を使用し、サーバ用の OS 3 3 を介して、サーバ固有のネットワークドライバ 3 4 を使用して、ハードウェア 3 5 を介して接続されているファイバケーブル 4 2、ATM スイッチ 4 5 を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバケーブル 4 6 に接続されているハードウェア 3 7 から、ファイル・マネージャ、ドライバ 3 8 によって、OS-9/OS-9000 3 9 上のダウンロードプロトコルである UPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステム RAM 1 0 に格納される。

【0130】ダウンロードされたデータは CPU モジュール 2 の暗号化モジュール 6 を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システム RAM 1 0 に保存される。次に復号され、システム RAM に保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、MPEG データ以外のデータはバスを通じてグラフィックモジュール 3 へ送信され、MPEG データはバスを介してデマルチプレクサシンクコントロール 1 6 へ受け渡される。デマルチプレクサシンクコントロール 1 6 に受け渡された MPEG データは、画像データと音声データの切り分け処理が行われ、同期をとって、MPEG モジュール 4 へ受け渡される。MPEG モジュール 4 に受け取られた画像データは MPEG ビデオプロセッサ 1 4 で、音声データは MPEG オーディオプロセッサ 1 5 でそれぞれ復号処理され、MPEG ビデオプロセッサ 1 4 で復号されたビデオ信号は、グラフィックモジュール 3 のオーバレイコントローラ 1 3 に受け渡され、MPEG オーディオプロセッサ 1 5 で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール 3 へ受け渡された静止画像データは静止画像プロセッサ 1 2 で復号処理され、オーバレイコントローラ 1 3 へ受け渡される。オーバレイコントローラ 1 3 では、静止画像プロセッサ 1 2 から受け取った静止画像データと MPEG ビデオプロセッサ 1 4 から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【0131】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図34と同様である。まず、デジタル双方向通信端末はシステムRAM内の暗号化データ記憶領域13に、送信すべきデータの暗号化されたデータの検索を行う。暗号化データ記憶領域13に送信すべきデータが存在しない場合、デジタル双方向通信端末はCPUモジュール2において、暗号化モジュール6を用いて暗号化鍵を生成する。次に、デジタル双方向通信端末は暗号化モジュール6によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール6を使用してサーバの公開鍵を用いて暗号化する。デジタル双方向通信端末は暗号化を施したデータと暗号化に使用した暗号化鍵をシステムRAM10上の暗号化データ記憶領域13に格納する。暗号化データ記憶領域の要領を超える場合には、最終の参照日時が最も古いものから順にデータを消去する。暗号化データ記憶領域13に送信すべきデータが存在する場合、デジタル双方向通信端末はそのデータと暗号化鍵をサーバに送信する。

【0132】次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール5の制御チャンネルI/Fへ送られ、制御チャンネルI/Fを介して、同軸ケーブル44、ファイバーバックボーン43を経由して、サーバに送信される。データの送信は図9と同様に、OS-9/OS-90039上のダウンロードプロトコルであるUPLINK/DOWNLINK API 40を使用し、ファイル・マネージャ、ドライバ38によって、サーバ用のOS33を介して、ファイバーケーブル42に接続されているハードウェア37から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API 32を使用して、サーバ固有のネットワークドライバ34を使用して、ハードウェア35を介して接続されているファイバーケーブル46からATMスイッチ45を経由してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またデジタル双方向通信端末におけるデータの暗号化処理の必要回数を減らすことが可能となり、サーバへのデータ送信の効率を上げることが可能となる。

【0133】

【発明の効果】本発明は以上説明したように構成されて

いるので、以下に示すような効果を奏する。

【0134】デジタル双方向通信端末にデジタル双方向通信システムのダウンロード機能を利用した暗号化機能の実現が可能となり、デジタル双方向通信端末に暗号化機能を実現することによって、よりセキュリティを必要とするサービスの提供が可能である。加えて、データと同様にアプリケーションをダウンロードすることが可能であり、更にダウンロードされたアプリケーションをダイナミックに動作可能とするOS/9の特徴を利用することによって、デジタル双方向通信端末本体に特別な変更を加えることなく暗号化機能を付加することが可能となり、また暗号化機能の更新を容易に実現する。

【0135】また、デジタル双方向通信端末とサーバの間で授受されるデータを暗号化することによって、盗聴によるデータの保護は実現できるが、送った情報が途中で故意に変更され、送った内容と異なる内容が相手に届く恐れのあるデータの改ざん、第三者によって正当なユーザあるいはサーバのふりをして誤った情報をおくるなりすましの脅威は存在する。従って、認証機能のH/Wによる実装を行うことによって、データを改ざん、なりすましから保護し、よりセキュリティ機能の強化が実現できる。

【0136】また、認証機能のS/Wによる実装を行うことによって、より強化されたセキュリティ機能を実現しつつ、コストを削減できる。

【0137】また、データの保護機能を付加するための暗号化・復号化には複雑な演算が必要とされるため、特にセキュリティの確保を必要とするデータを選択的に暗号化・復号化する機能を付加することによって、デジタル双方向通信端末の負荷を軽減し、サーバとのデータ授受の速度を上げることができる。

【0138】また、データが暗号化・復号化を必要とするか否かをサーバ側で決定し、そのリストをデジタル双方向通信端末にダウンロードしてサーバ側と端末側で共通のリストによって、暗号化・復号化を選択的に実行する機能を有することによって、ユーザの操作が不要となり、ユーザの操作の煩雑さをなくすと共に、ユーザによる誤操作の危険性を回避する効果がある。さらに暗号化・復号化は共通なリストによって選択するため、データが暗号化されたものであるかどうかを示すフラグを送受信されるデータに付加する必要がなくなる。

【0139】また、デジタル双方向通信端末からサーバへ送信するデータで、暗号化されたものを保持しておくことによって、同じデータを何度も暗号化する必要がなくなり、デジタル双方向通信端末の負荷を軽減し、動作速度を上げることができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態1であるシステム構成を示すブロック図である。

【図2】 デジタル双方向通信端末電源ON時のフロー

チャートである。

【図 3】 データダウンロード時のフローチャートである。

【図 4】 データ送信時のフローチャートである。

【図 5】 電話回線を介したサーバとデジタル双方向通信端末の接続図である。

【図 6】 本発明の実施の形態 2 であるシステム構成を示すブロック図である。

【図 7】 HFC 方式によるサーバとデジタル双方向通信端末の接続図である。

【図 8】 本発明の実施の形態 3 であるシステム構成を示すブロック図である。

【図 9】 ATM によるサーバとデジタル双方向通信端末の接続図である。

【図 10】 本発明の実施の形態 4 であるシステム構成を示すブロック図である。

【図 11】 デジタル双方向通信端末電源 ON 時のフローチャートである。

【図 12】 データダウンロード時のフローチャートである。

【図 13】 データ送信時のフローチャートである。

【図 14】 本発明の実施の形態 5 であるシステム構成を示すブロック図である。

【図 15】 本発明の実施の形態 6 であるシステム構成を示すブロック図である。

【図 16】 本発明の実施の形態 7 であるシステム構成を示すブロック図である。

【図 17】 本発明の実施の形態 8 であるシステム構成を示すブロック図である。

【図 18】 本発明の実施の形態 9 であるシステム構成を示すブロック図である。

【図 19】 本発明の実施の形態 10 であるシステム構成を示すブロック図である。

【図 20】 デジタル双方向通信端末電源 ON 時のフローチャートである。

【図 21】 データダウンロード時のフローチャートである。

【図 22】 データ送信時のフローチャートである。

【図 23】 本発明の実施の形態 11 であるシステム構成を示すブロック図である。

【図 24】 本発明の実施の形態 12 であるシステム構

成を示すブロック図である。

【図 25】 本発明の実施の形態 13 であるシステム構成を示すブロック図である。

【図 26】 デジタル双方向通信端末電源 ON 時のフローチャートである。

【図 27】 データダウンロード時のフローチャートである。

【図 28】 データ送信時のフローチャートである。

【図 29】 本発明の実施の形態 14 であるシステム構成を示すブロック図である。

【図 30】 本発明の実施の形態 15 であるシステム構成を示すブロック図である。

【図 31】 本発明の実施の形態 16 であるシステム構成を示すブロック図である。

【図 32】 デジタル双方向通信端末電源 ON 時のフローチャートである。

【図 33】 データダウンロード時のフローチャートである。

【図 34】 データ送信時のフローチャートである。

【図 35】 本発明の実施の形態 17 であるシステム構成を示すブロック図である。

【図 36】 本発明の実施例の形態 18 であるシステム構成を示すブロック図である。

【図 37】 従来の ROM のメモリマップである。

【図 38】 従来のデジタル双方向通信端末における電源 ON 時のフローチャートである。

【図 39】 従来のデジタル双方向通信端末におけるデータダウンロード時のフローチャートである。

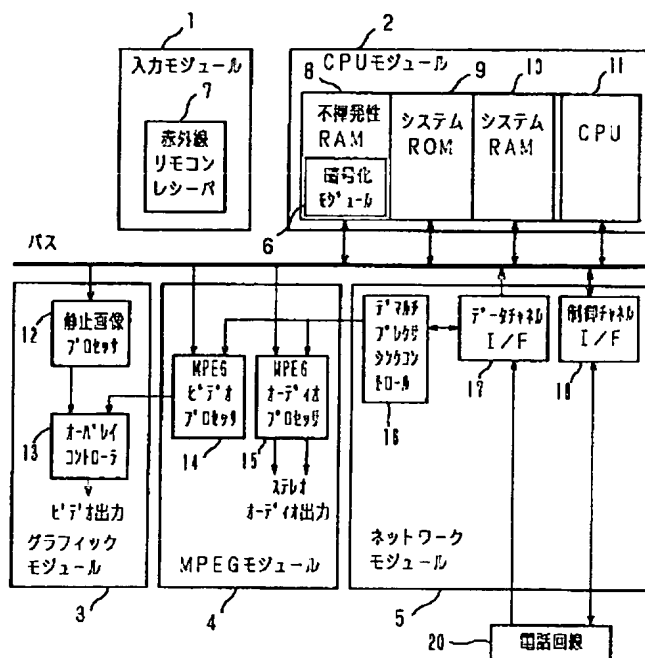
【図 40】 OS/9 を核とした従来のデジタル双方向通信端末の構成図である。

【符号の説明】

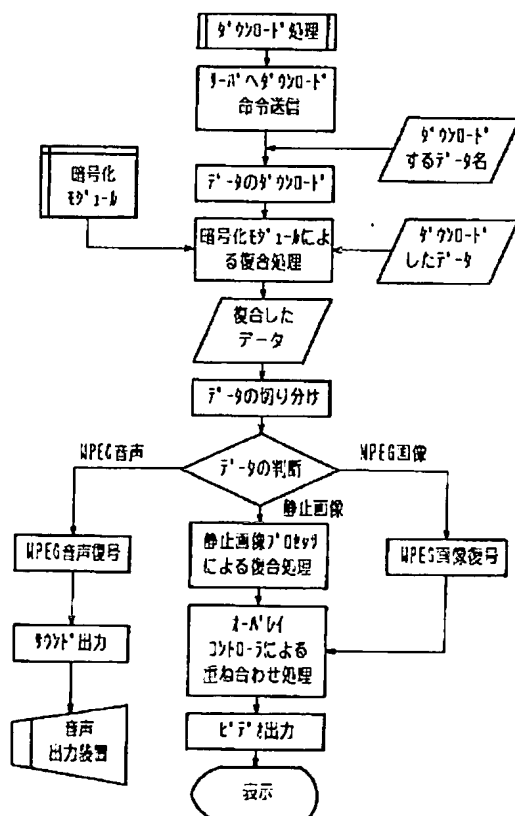
1 入力モジュール、2 CPUモジュール、3 グラフィックモジュール、4 MPEGモジュール、5 ネットワークモジュール、6 暗号化モジュール、7 赤外線リモコンレシーバ、8 不揮発性 RAM、9 システム ROM、10 システム RAM、11 CPU、12 静止画像プロセッサ、13 オーバレイコントローラ、14 MPEGビデオプロセッサ、15 MPEGオーディオプロセッサ、16 デマルチプレクサコントロール、17 データチャネル I/F、18 制御チャネル I/F。



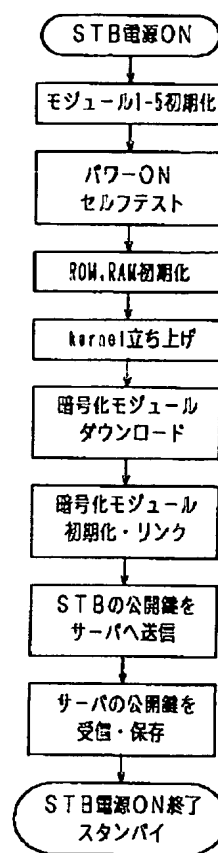
【図1】



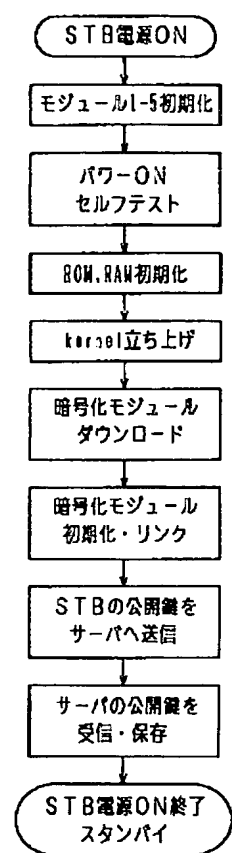
【図3】



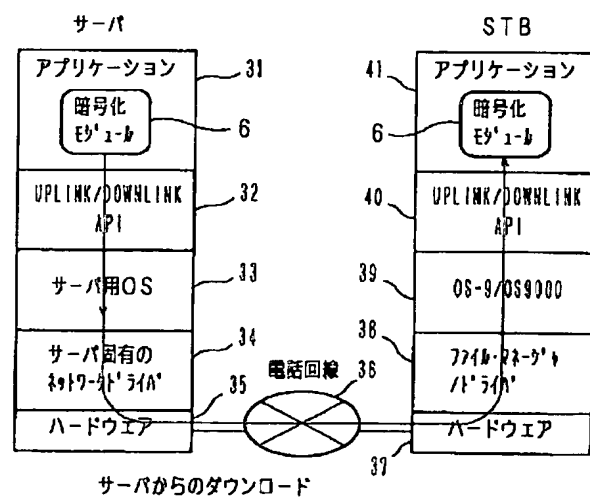
【図2】



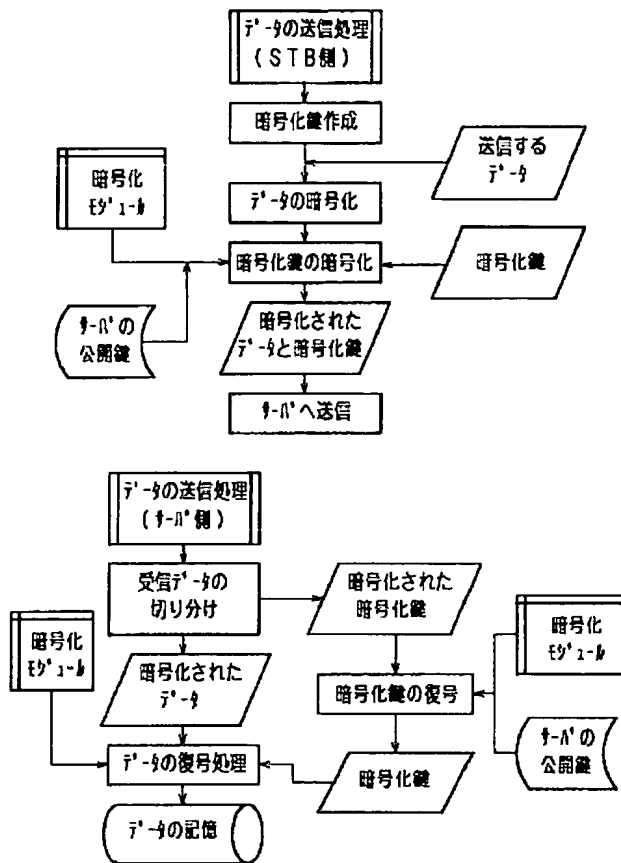
【図20】



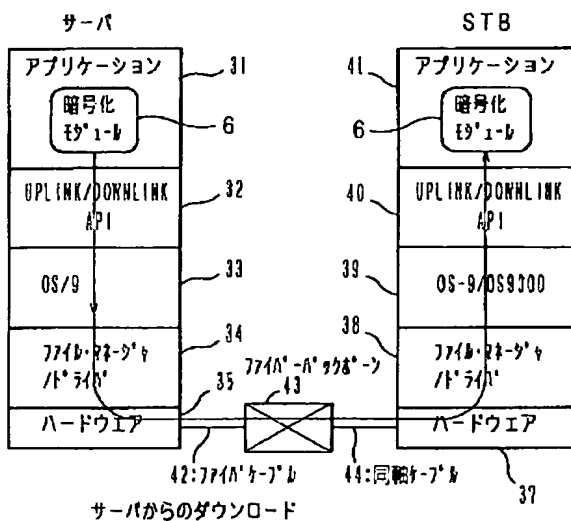
【図5】



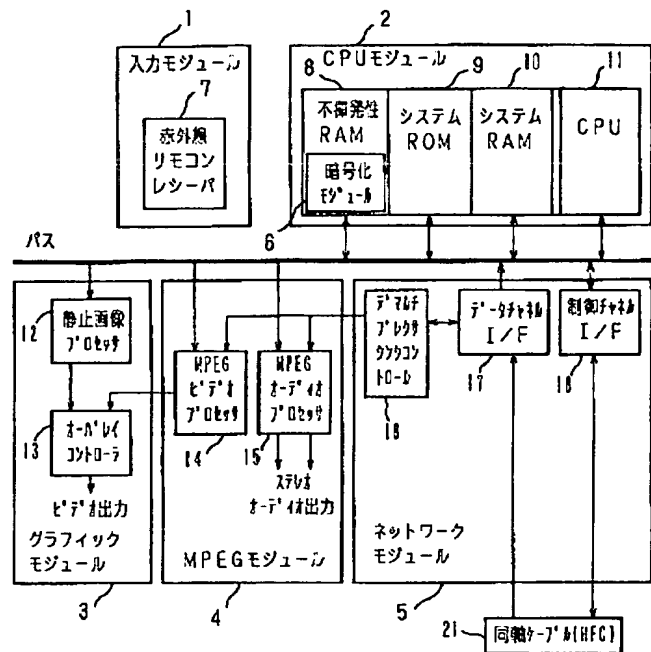
【図4】



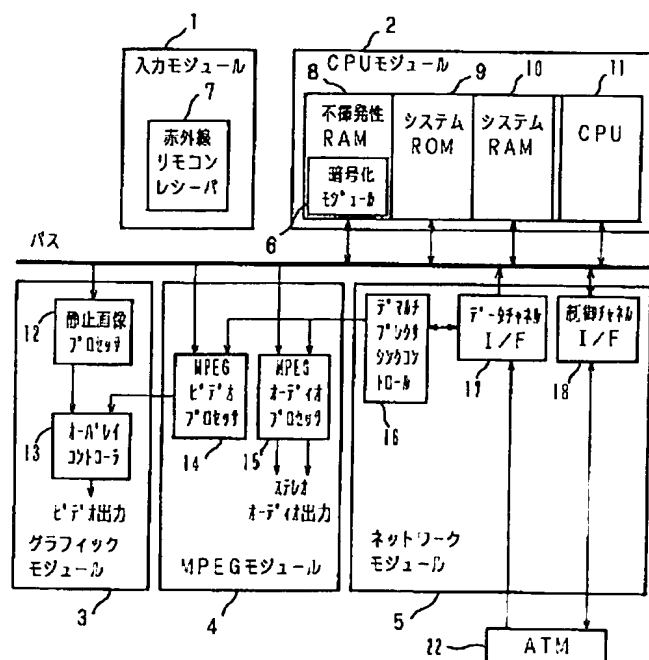
【図7】



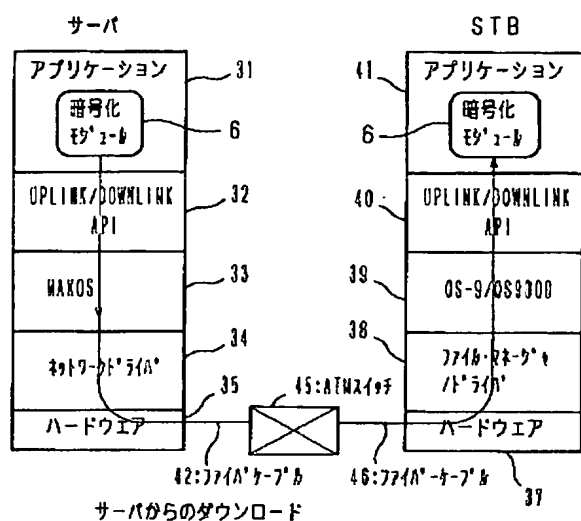
【図6】



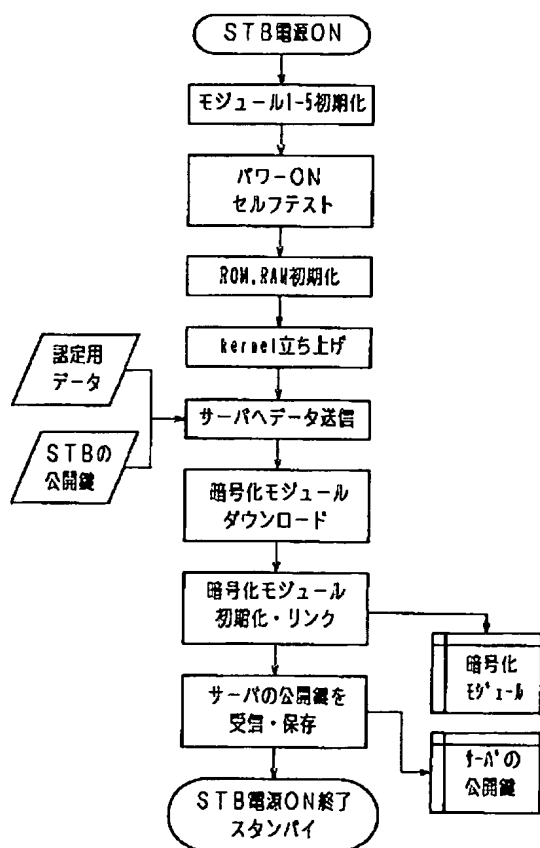
【図8】



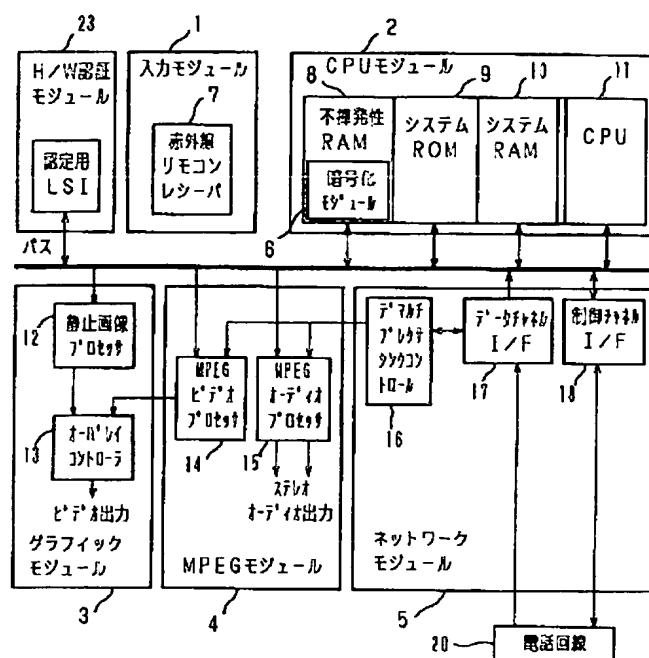
【図9】



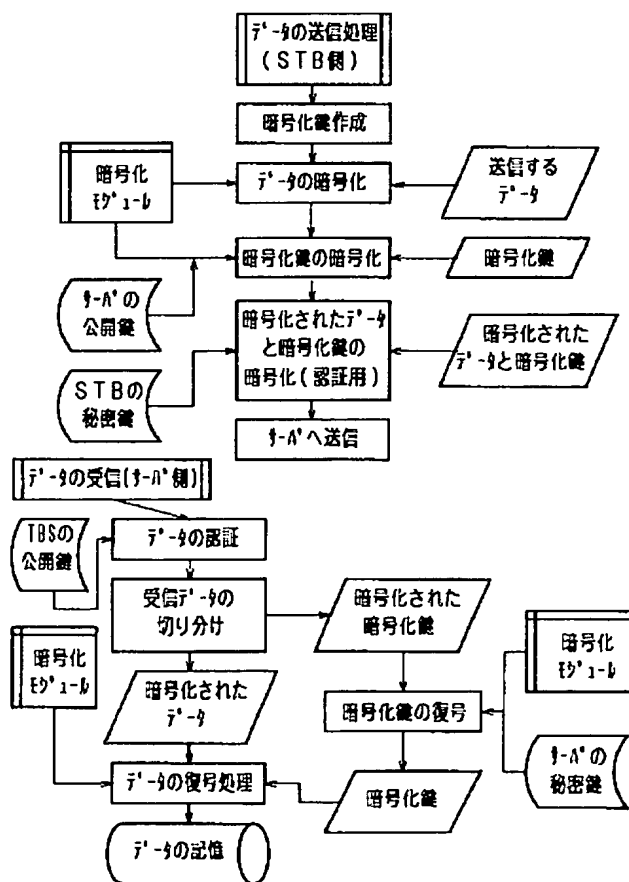
【図11】



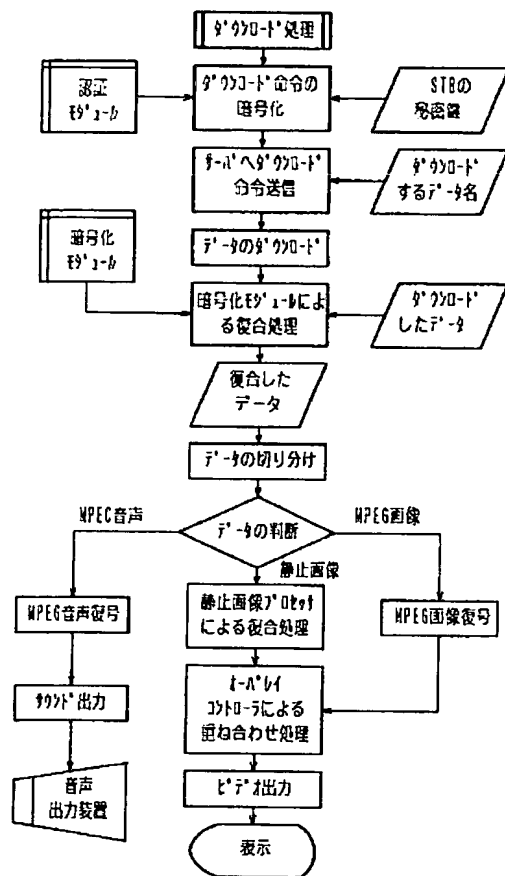
【図10】



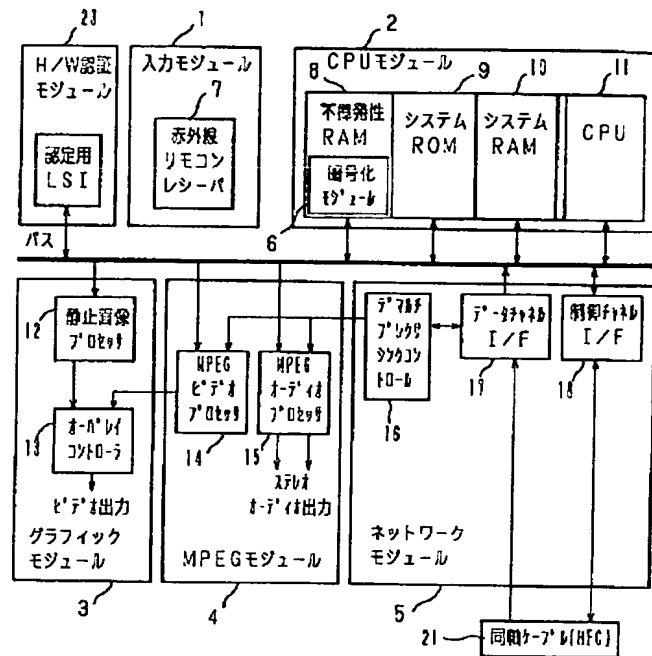
【図13】



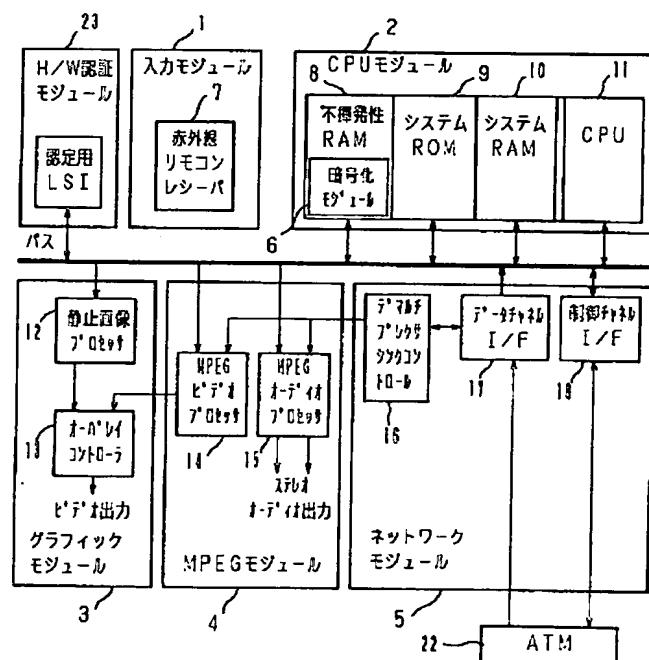
【図 1 2】



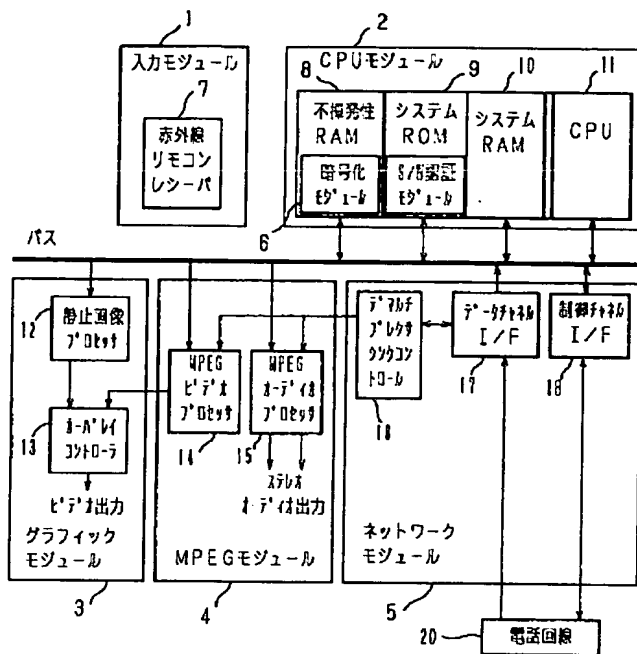
【図 1 4】



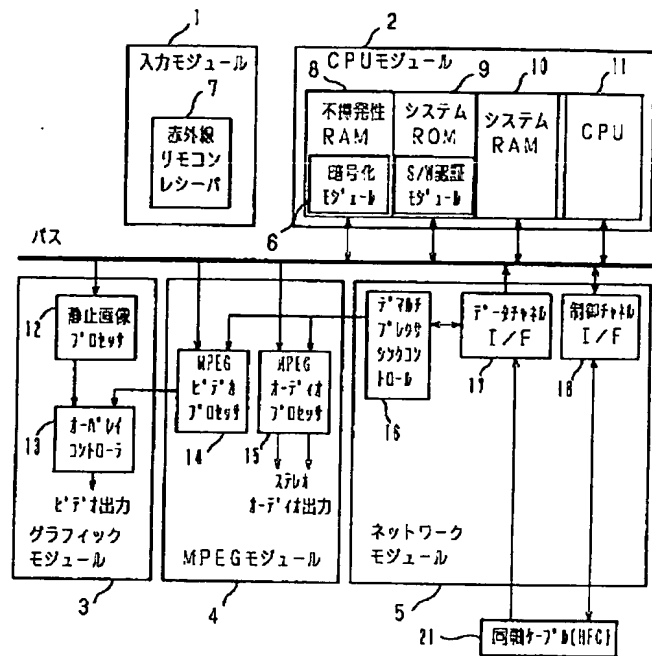
【図 1 5】



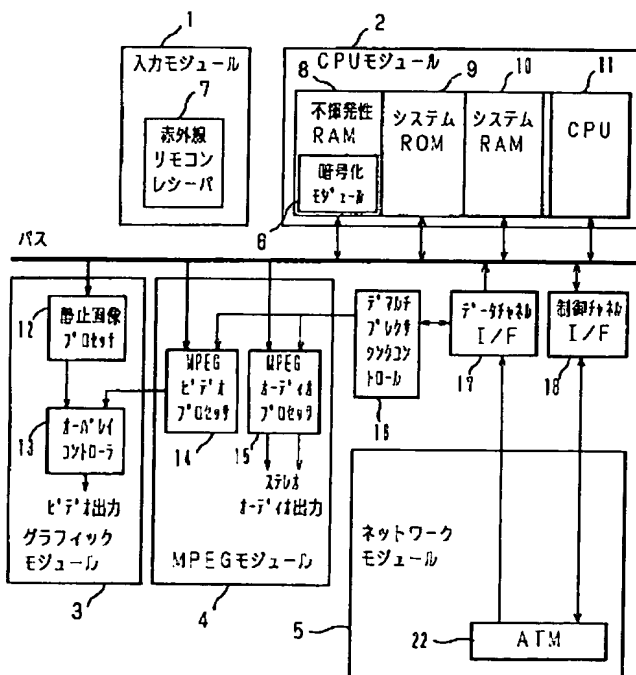
【図16】



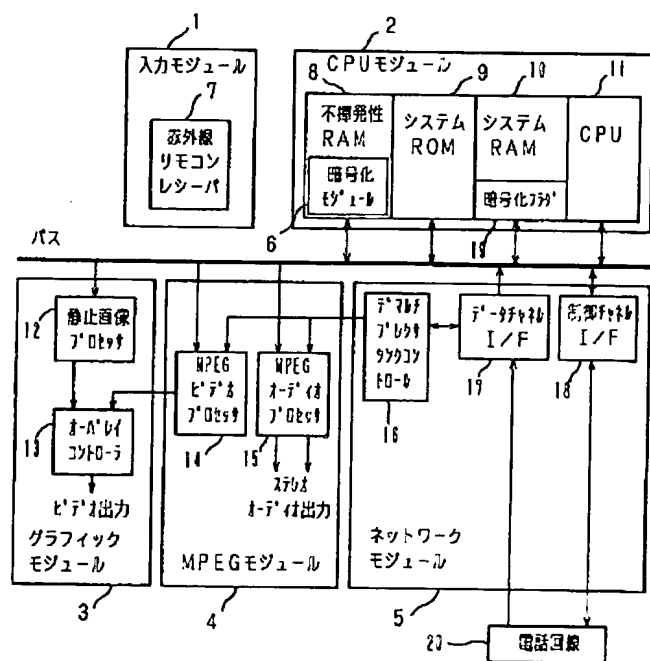
【図17】



【図18】

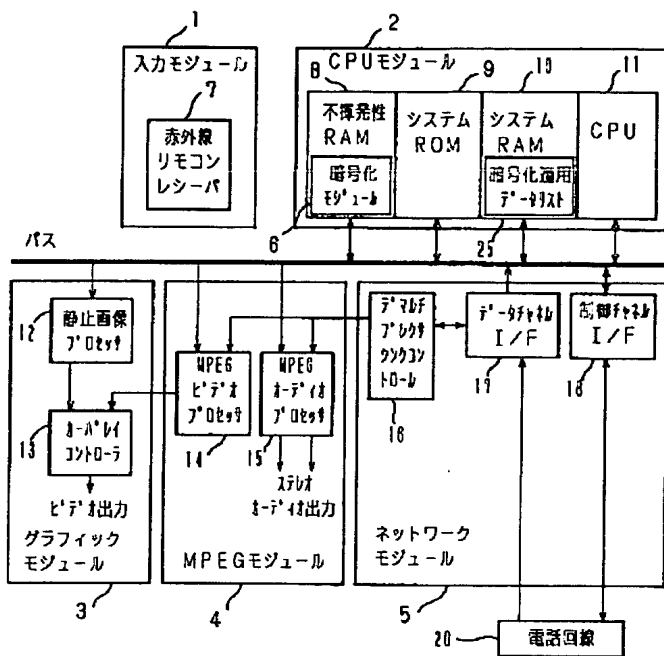


【図19】

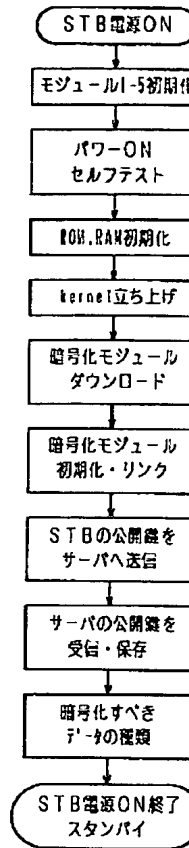




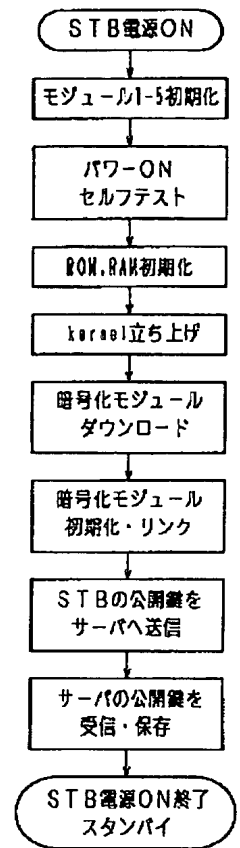
【図25】



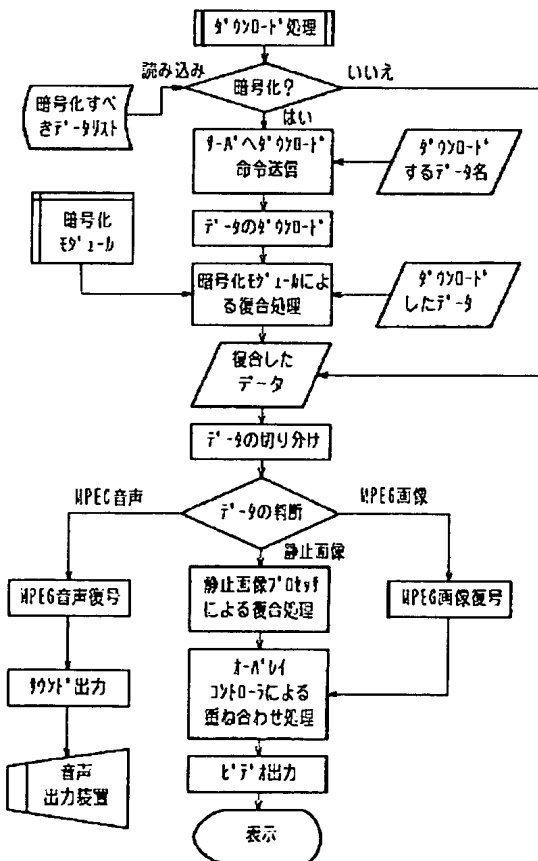
【図26】



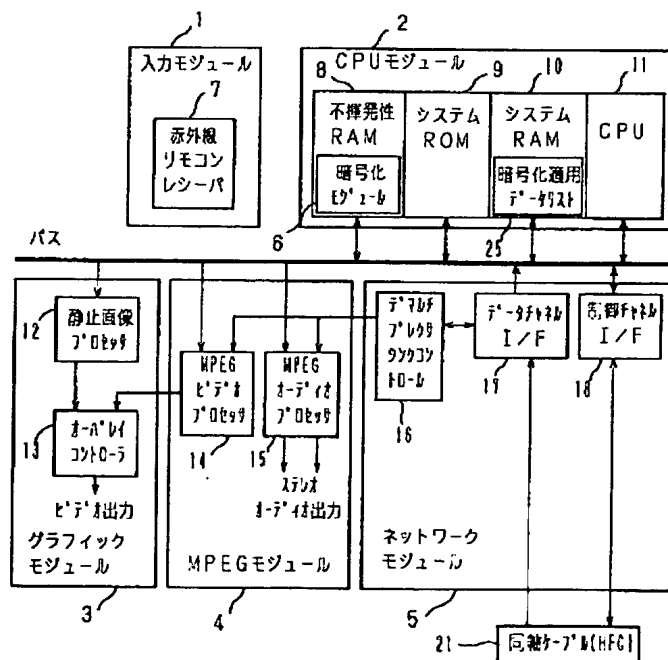
【図32】



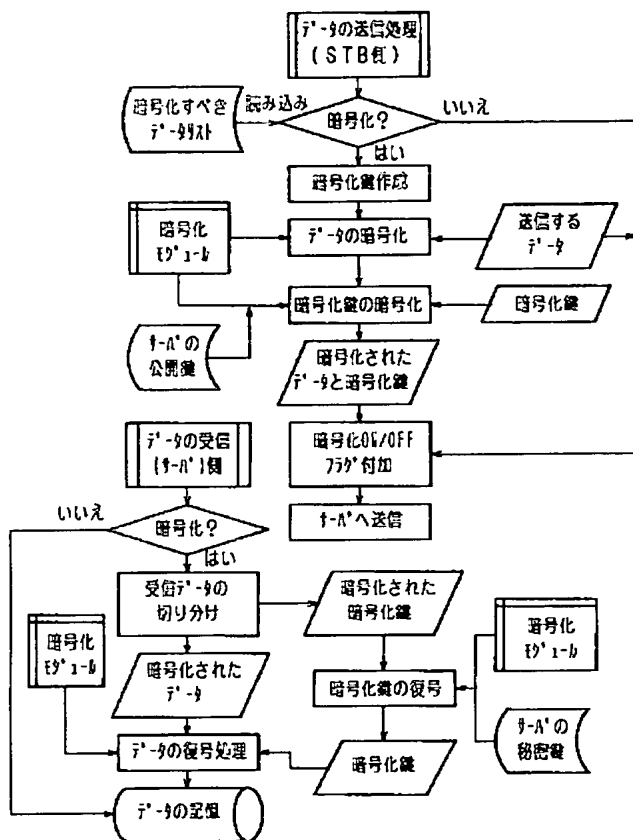
【図27】



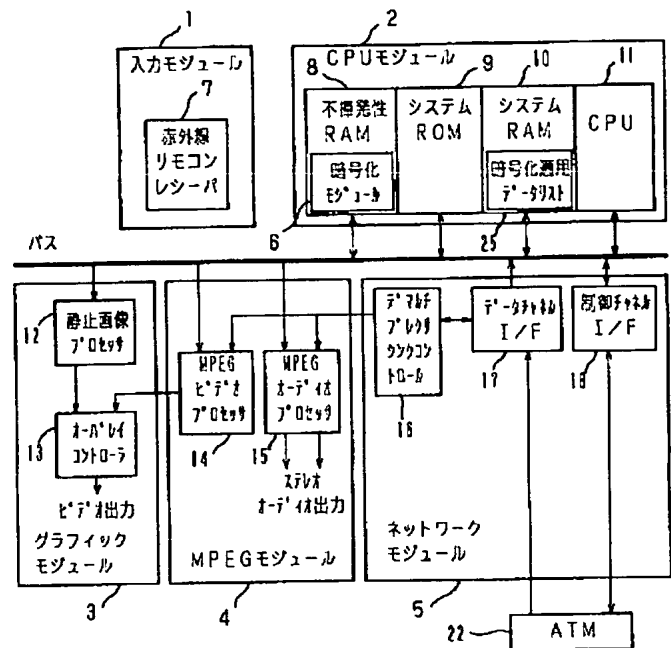
【図29】



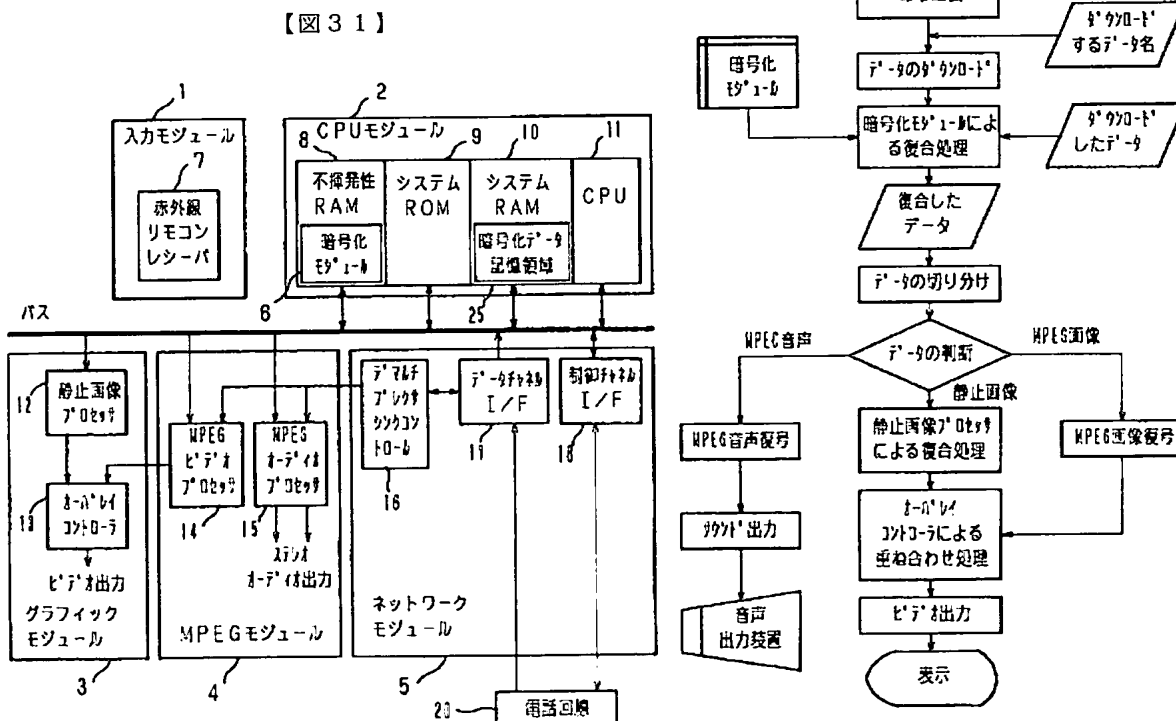
【圖 28】



【図 30】

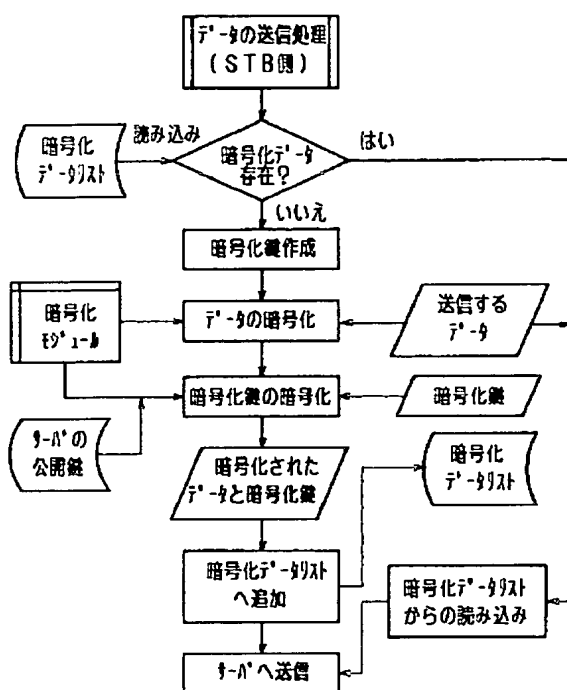


【例 3 3】

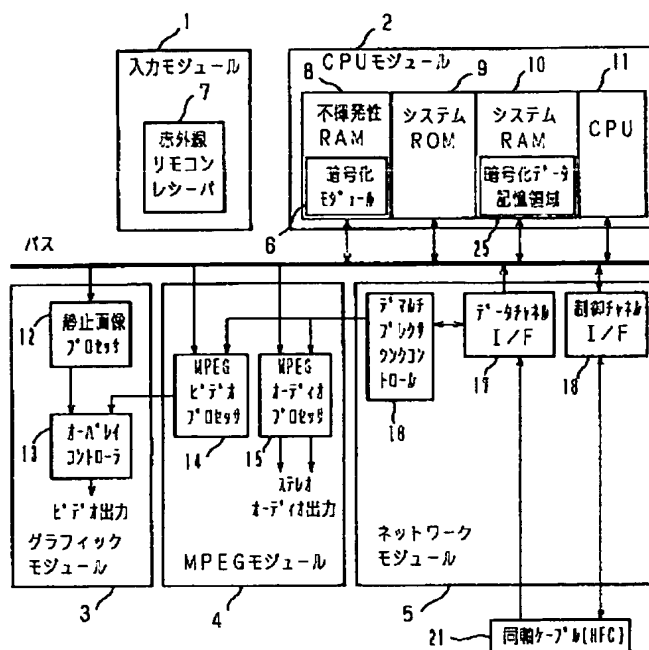




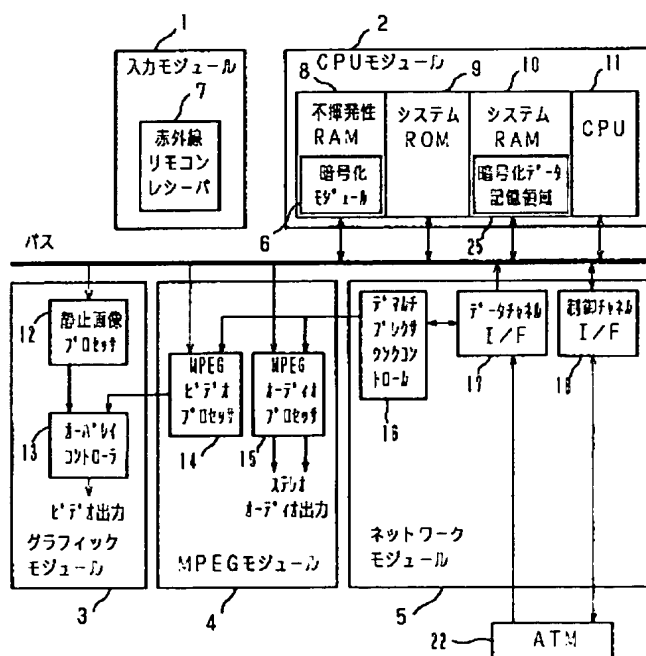
【例 3 4】



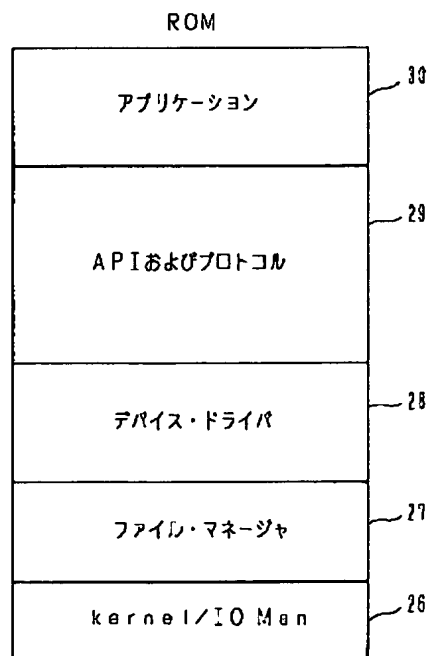
【図 35】



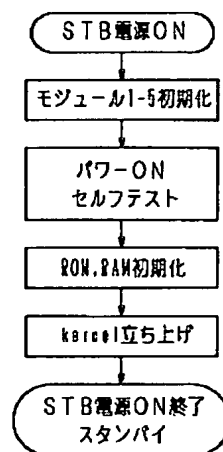
【図 3 6】



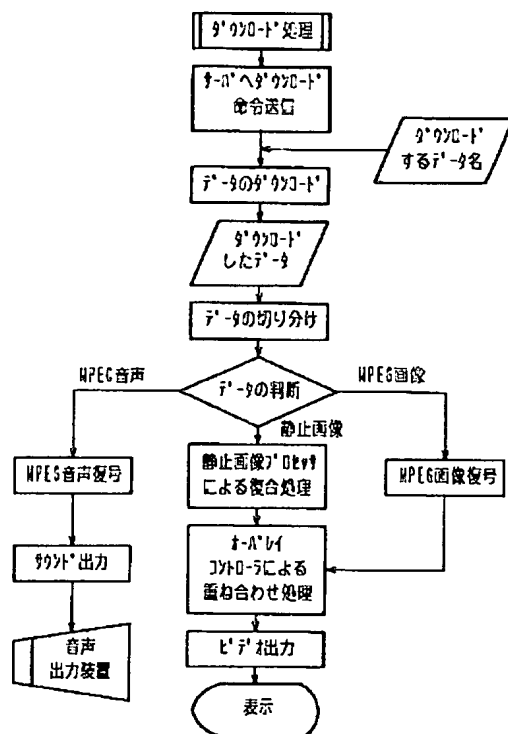
【例 3 7】



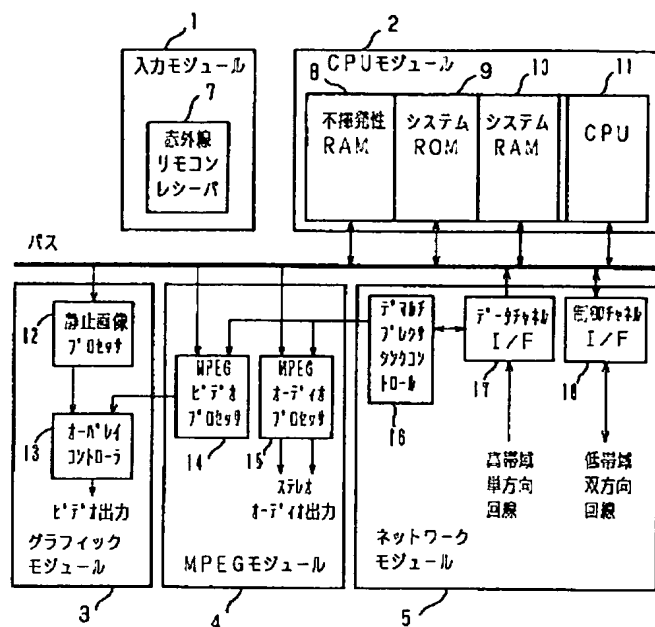
【图 38】



【図39】



【図40】



フロントページの続き

(51)Int.Cl. <sup>6</sup>		識別記号	庁内整理番号	F I	技術表示箇所	
G 0 9 C	1/00	6 6 0	7259-5 J	G 0 9 C	1/00	6 6 0 E
H 0 4 H	1/02			H 0 4 H	1/02	E
						F
H 0 4 L	9/08			H 0 4 N	7/14	
	9/32			H 0 4 L	9/00	6 0 1 C
H 0 4 N	7/14					6 0 1 E
	7/167					6 7 5 B
				H 0 4 N	7/167	Z